NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 22, 2009

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: ***North American Electric Reliability Corporation,***
Docket No.RM06-22-000

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits this filing in accordance with Section 215(d)(1) of the Federal Power Act ("FPA") and Part 39.5 of the Federal Energy Regulatory Commission's ("FERC" or the "Commission") regulations, seeking approval for proposed modifications to Critical Infrastructure Protection ("CIP") Reliability Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1 and CIP-009-1. The modified Reliability Standards are redesignated as CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, CIP-006-2, CIP-007-2, CIP-008-2 and CIP-009-2 and are contained in **Exhibit A** to this petition.

The modifications addressed by this filing are in direct response to the Commission's directives in Order No. 706, issued on January 18, 2008.[1] In that Order,

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, (Order No. 706), 122 FERC ¶ 61,040 (2008).

FERC approved the CIP Version 1 Reliability Standards and associated implementation plan but also directed NERC to develop modifications to CIP Reliability Standards CIP-002-1 through CIP-009-1 to address specific concerns identified by the Commission. The magnitude of the directives dictated by Order No. 706 resulted in a phased approach to addressing those directives. This filing represents the result of Phase 1 of the overall plan for revising the CIP Reliability Standards. Subsequent phases of the project for modifying the CIP Reliability Standards will address the remainder of the Commission's directives provided in Order No. 706 that are not addressed in this filing.

These proposed CIP Version 2 Reliability Standards were approved by the NERC Board of Trustees on May 6, 2009. NERC requests that, upon Commission approval, these CIP Version 2 Reliability Standards be made effective in accordance with the effective date provisions set forth in the proposed CIP Reliability Standards and associated implementation plan, and that upon the effective date of these Reliability Standards, the correlating Version 1 Cyber Security Reliability Standards be retired.

NERC's petition consists of the following:

- this transmittal letter;
- a table of contents for the entire petition;
- a narrative description of the necessary modifications describing how the resulting proposed CIP Reliability Standards fulfill the Commission's directives;
- CIP Reliability Standards CIP-002-2 through CIP-009-2 submitted for approval (**Exhibit A**);
- the complete Development Record of the proposed CIP Reliability Standards (**Exhibit B**);
- the Cyber Security Standard Drafting Team Roster (**Exhibit C**); and
- CIP Reliability Standards Redline/Strikeout Version showing the Proposed Changes to Version 1 Standards (**Exhibit D**).

Please contact me if you have any questions regarding this filing.

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins

Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	) **) Docket No. RM06-22-000** **)**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF VERSION 2 CRITICAL INFRASTRUCTURE PROTECTION STANDARDS

Rick Sergel
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

May 22, 2009

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby requests that the Federal Energy Regulatory Commission (the "Commission" or "FERC") approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA") and Section 39.5 of the Commission's regulations, 18 C.F.R. § 39.5,[1] eight Critical Infrastructure Protection ("CIP") Reliability Standards, CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, CIP-006-2, CIP-007-2, CIP-008-2 and CIP-009-2 (the "Version 2 CIP Reliability Standards," or "Version 2 Standards"). These Version 2 Standards contain modifications to CIP Reliability Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1 and CIP-009-1 (the "Version 1 CIP Reliability Standards," or "Version 1 Standards"), consistent with Commission directives in Order No. 706, issued on January 18, 2006.[2]

In Order No. 706, the Commission approved the Version 1 CIP Reliability Standards but directed NERC to develop modifications to the Version 1 Standards to address specific concerns identified by the Commission.[3] The Version 2 Standards presented herein were developed in accordance with NERC's *Reliability Standards Development Procedure* and represent Phase 1 efforts to comply with the Commission's directives provided in Order No. 706. These Version 2 Standards were approved by the NERC Board of Trustees on May 6, 2009. Upon Commission approval, these proposed Version 2 CIP Reliability Standards are intended to supersede the existing Commission-approved Version 1 CIP Reliability Standards.

---

[1] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005) (codified at 16 U.S.C. §824o (2007)).
[2] *Mandatory Reliability Standards for Critical Infrastructure Protection*, (Order No. 706) 122 FERC ¶ 61,040 (2008).
[3] *See* Order No. 706 at P 1.

NERC is not requesting approval for revised Violation Risk Factors ("VRFs") or Violation Severity Levels ("VSLs") with this filing, but will request approval of revised VRFs and VSLs that will be submitted in a filing to the Commission no later than December 31, 2009.

Exhibit A to this filing sets forth the proposed Version 2 CIP Reliability Standards. **Exhibit B** contains the complete development record for the proposed Version 2 Standards. This record includes the Standard Authorization Request ("SAR"), the ballot pool, the final ballot results by registered ballot body members, stakeholder comments received during the development of these Reliability Standards, and an explanation of how those comments were considered in revising the CIP Reliability Standards. **Exhibit C** contains the roster identifying the members of the Cyber Security Standard Drafting Team that developed the proposed Version 2 Standards. **Exhibit D** contains a redline/strikeout version showing the changes made to the Version 1 CIP Reliability Standards to develop the Version 2 Standards. NERC also is filing these proposed Reliability Standards and associated implementation plans with applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

Rick Sergel
President and Chief Executive Officer
David N. Cook*
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael*
Assistant General Counsel
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net

*Persons to be included on the Commission's service list are indicated with an asterisk.

III. BACKGROUND

A. Regulatory Framework

Through its enactment of the Energy Policy Act of 2005 (the "Energy Policy Act"), Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk electric system, and with the duties of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval.[4] Section 215 of the Energy Policy Act provides that all users, owners and operators of the bulk electric system in the United States will be subject to the Commission-approved Reliability Standards.

[4] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005) (codified at 16 U.S.C. §824o (2007)).

On February 3, 2006, the Commission issued Order No. 672,[5] which established a process to select and certify an Electric Reliability Organization (ERO), and subsequently, the Commission certified NERC as the ERO.[6] Pursuant to Section 215 of the FPA, the ERO is charged with developing mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Upon approval by the Commission, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or the Commission can independently enforce these Reliability Standards.

On August 28, 2006, NERC submitted to the Commission for approval Reliability Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1 and CIP-009-1.[7] These eight CIP Reliability Standards were approved in the Commission's Order No. 706 along with NERC's implementation plan that set milestones for responsible entities to achieve full compliance with the CIP Reliability Standards.[8] In Order No. 706, the Commission directed NERC to develop modifications to the CIP Reliability Standards through its reliability standards development process to address specific concerns identified by the Commission.[9] The Version 2 CIP Reliability Standards presented in this filing represent NERC's Phase 1 efforts to comply with the

[5] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 71 FR 8662 (February 17, 2006), FERC Stats. & Regs. ¶ 31,204 (2006), *order on reh'g*, Order No. 672-A, 71 FR 19814 (April 18, 2006), FERC Stats. & Regs. ¶ 31,212 (2006).

[6] *North American Electric Reliability Corporation*, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing," 116 FERC ¶ 61,062 (2006).

[7] *See North American Electric Reliability Council, et al.*, "Petition of the North American Electric Reliability Council and North American Electric Reliability Corporation for Approval of Proposed Reliability Standards," *Docket No. RM06-16-000* (August 28, 2006).

[8] Order No. 706 at PP 1 and 13.

[9] Order No. 706 at P 30. The Commission stated that "*any modification to a Reliability Standard, including a modification that addresses a Commission directive, must be developed and fully vetted through NERC's Reliability Standard development process.*"

Commission's directives provided in Order No. 706. Subsequent phases of the project for modifying the CIP Reliability Standards will address the remainder of the Commission's directives provided in Order No. 706 which are not addressed in this filing. Specifically, the following proposed changes included in Order No. 706 are addressed by this filing:

- removal of the term "reasonable business judgment" from the purpose section of each Reliability Standard;
- where applicable, removal of the phrase "acceptance of risk" from each Reliability Standard;
- revision to R4 in Reliability Standard CIP-002-2 to specify that the senior manager must annually approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets;
- revision to the Applicability section of Reliability Standard CIP-003-2 to require that all Responsible Entities must comply with R2 of Reliability Standard CIP-003-2;
- revision to R2 of Reliability Standard CIP-003-2 to specify that a single manager with overall responsibility and authority be designated;
- revision to R2.3 in Reliability Standard CIP-003-2 to specify that delegations of authority must be documented;
- revision to R1 in Reliability Standard CIP-004-2 to clarify that the Responsible Entity shall establish, document, implement, and maintain, a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices;
- revision to R2 in Reliability Standard CIP-004-2 to specify that all employees with authorized access must be trained prior to access, except in specified circumstances such as an emergency;
- revision to R2 in Reliability Standard CIP-004-2 to clarify that the Responsible Entity shall establish, document, implement, and maintain, an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets;
- revision to R3 in Reliability Standard CIP-004-2 to clarify that the Responsible Entity shall have a documented personnel risk assessment

program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, prior to personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets;

- revision to R2.3 in Reliability Standard CIP-005-2 to clarify that the Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s);

- revision to R1 in Reliability Standard CIP-006-2 to clarify that the Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s);

- revision to the Purpose statement in Reliability Standard CIP-007-2 to clarify that Responsible Entities will define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s);

- revision to the Implementation Plan for the Version 2 CIP Reliability Standards to clarify the formula to determine the "effective date" of the standards for each stakeholder and to provide an example of the calculation; and

- update to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to identify the schedule for becoming compliant with the requirements of the Version 2 CIP Reliability Standards and their successor standards, once an Entity's applicable 'Compliant' milestone date listed in the existing Version 1 Implementation Plan has passed.

B. Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC *Reliability Standards Development Procedure*, which is incorporated into the NERC Rules of Procedure as Appendix 3A.[10] In the ERO Certification Order, the Commission found that NERC's

[10] *See* NERC's *Reliability Standards Development Procedure Version 6.1*, Approved by the NERC Board of Trustees on March 12, 2007, and Effective June 7, 2007 ("*Reliability Standards Development Procedure*"), available at http://www.nerc.com/files/Appendix3A_StandardsDevelopmentProcess.pdf.

proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards.[11]

The development process is open to any person or entity with a legitimate interest in the reliability of the bulk power system. NERC's Standards Committee appoints Standard Drafting Teams ("SDT") to develop new or revisions to existing Reliability Standards. The SDT considers the comments of all stakeholders in the Reliability Standards development process, and an affirmative vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard for submission to the Commission. The proposed CIP Reliability Standards provided in **Exhibit A** were developed in accordance with this procedure.

C. Developmental History of the CIP Reliability Standards

In response to the Commission's directives in Order No. 706 to revise certain aspects of the CIP Reliability Standards, a Cyber Security SDT was appointed by the NERC Standards Committee on August 7, 2008 to support the project designated as Project 2008-06 CyberSecurity Order 706. The SDT was assigned the responsibility of reviewing and modifying each of the CIP Reliability Standards to ensure that they address the Order No. 706 directives and conform to the latest version of the ERO Rules of Procedure, including the *Reliability Standards Development Procedure*.

The extensive scope of Project 2008-06 in responding to Order No. 706 led the Cyber Security SDT to develop a multiphase strategy to revise the CIP Reliability Standards and the associated implementation plan for these standards. The work reflected in this filing represents Phase 1 of that work plan. Phase 1 includes some of the

[11] Order 672 PP 268, 270.

necessary modifications to the CIP-002-1 through CIP-009-1 Reliability Standards directed by Order No. 706. Those modifications to the CIP Reliability Standards directed by the Commission in Order No. 706 that are not included in this filing will be addressed in later phases of the work plan for Project 2008-06 Cyber Security Order No. 706 and will be filed with the Commission at a later time.

The SDT's initial meeting took place in October 2008, with monthly meetings thereafter. WebEx and conference calls were scheduled in between meetings. As a result of these meetings, the SDT: (a) prepared the initial Phase 1 revisions to the existing CIP Reliability Standards; (b) prepared the revisions to the associated implementation plan for those standards; and (c) agreed on an Implementation Plan for newly identified Critical Cyber Assets.

The Version 2 CIP Reliability Standards and associated documents were posted for industry comment on November 21, 2008, for a 45-day comment period that lasted through January 5, 2009. The SDT met on January 7, 2009 through January 9, 2009 to perform a preliminary review of the comments, discuss the strategy and logistics for preparation of the responses and resultant changes to the posted documents, and to begin drafting the Consideration of Comments Report for the posting. There were approximately 125 pages of comments received from 52 commenters representing individuals and group responses from a broad cross-section of the industry. Comments were received from representatives of 9 of the 10 defined Industry Segments.

The revised Version 2 CIP Reliability Standards were then posted for a 30-day pre-ballot industry review period on March 3, 2009. NERC conducted the initial ballot of the Version 2 CIP Reliability Standards from April 1, 2009 through April 10, 2009.

The proposed Version 2 CIP Reliability Standards achieved a weighted segment affirmative vote of 84.06% on the initial ballot with 91.90% of those who joined the ballot pool returning a ballot. There were 39 negative ballots submitted with 24 submitted with comment. The responses from the SDT to the initial negative ballots with comment were posted on April 17, 2009, and the recirculation ballot was held from April 17, 2009 through April 27, 2009. The final ballot resulted in a weighted segment affirmative vote of 88.32%, with 94.37% of the ballot pool casting ballots. The NERC Board of Trustees reviewed and approved the revisions to the Version 2 CIP Reliability Standards on May 6, 2009.

IV. PROPOSED MODIFICATIONS TO CIP RELIABILITY STANDARDS

Based on FERC Directives from Order No. 706 and stakeholder comments, and to conform to the latest templates for Reliability Standards, NERC proposes the following general modifications to the CIP Reliability Standards (CIP-002 through CIP-009) and associated implementation plan:

- Removal of Specific Terminology:[12]
  - From the Purpose Section: Removal of the term "reasonable business judgment."
  - Where applicable, removal of the phrase "acceptance of risk."

- Versions:
  - Phase 1 changes to the existing Version 1 Standards will be reflected as CIP-002-2 through CIP-009-2.

- The Effective Date section has been updated to incorporate the proposed implementation timeframe for CIP-002-2 through CIP-009-2.

- Administrative edits have been made to reflect changes in numbering references.

- Requirements Numbering Formats:

[12] Order No. 706 at P 14.

- Requirements that present options for compliance have been identified with bullets in lieu of numbers.

- Measures:
  - The format of the Measures was modified to conform to the current format used in other Reliability Standards.

- Compliance Elements:
  - The compliance elements of the standards were updated to reflect the language used in the ERO Rules of Procedure.
  - The term, "Compliance Monitor" was replaced with "Compliance Enforcement Authority."
  - The term, "Regional Reliability Organization" was replaced with "Regional Entity."
  - The Compliance Monitoring and Enforcement Processes were added.
  - The Monitoring Time Period and Reset Periods were marked as "not applicable."
  - The Data Retention section was updated.

In addition to the general modifications noted above for all Version 2 CIP Reliability Standards, the following specific modifications are proposed to apply to particular CIP standards:

CIP-002-2 Critical Cyber Asset Identification

- As directed in Order No. 706:[13]
  - R4 Annual Approvals: Add that the senior manager shall annually review and approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets as required in prior version.

CIP-003-2 Security Management Controls

- Simplification:
  - R2.1 Leader Identification: Remove the need for business phone and business address designation.

- As directed in Order No. 706:
  - Applicability 4.2.3: Requires Responsible Entities having no Critical Cyber Assets to comply with CIP-003-2 R2.

[13] Order No. 706 at P 294

- R2 Leadership: Require the designation of a single manager, with overall responsibility and authority for leading and managing the entity's implementation of CIP. The word "authority" is an addition.

- R2.3 Permits the assigned senior manager to delegate authority in writing for specific actions, where allowed, throughout the CIP standards.

CIP-004-2 Personnel and Training

- Clarification to ensure that requirement must be implemented:
  - R1 Awareness: Explicitly requires implementation of Awareness Program.
  - R2 Training: Explicitly requires implementation of the Training Program.

- As directed in Order No. 706:
  - R2.1 Training: Personnel having access to Critical Cyber Assets must be trained prior to their being granted such access, except in specified circumstances, such as an emergency. This replaces the allowance for 90 days to complete the training and adds a provision for emergency situations.
  - R3 Personnel Risk Assessment: Personnel risk assessment shall be conducted prior to granting personnel access to Critical Cyber Assets except in specified circumstance such as an emergency. This replaces the allowance for 30 days to complete personnel risk assessment and adds a provision for emergency situations.

CIP-005-2 Electronic Security Perimeter(s)

- Clarification:
  - Clarifies the scope of this requirement to include Cyber Assets used in either access control and/or monitoring to the Electronic Security Perimeter.
- Clarification to ensure that requirement must be implemented:
  - R2.3 Electronic Access Controls: Explicitly requires the implementation of the procedure to secure dial-up access to the Electronic Security Perimeter.

CIP-006-2 Physical Security

- Restructuring of Requirements:
  - Former requirement R1.8 moved and incorporated into new Requirement R2 (Protection of Physical Access Control Systems) as Requirement R2.2.
  - Other modifications to Requirements R1.1 through R1.8 for readability.

- Clarifications to ensure that the following requirement must be implemented:
  - R1 through R1.8 Physical Security Plan: All requirements of the Physical Security Plan must be implemented.

- Additional Clarifications:
  - R1.6 Escorted Access: Clarified that the escort within a Physical Security Perimeter should continually remain with the escorted person.
  - R1.8 Annual Review: Formerly Requirement R1.9.
  - R2.2 (Formerly R1.8.) Changed references to requirement numbers as appropriate.
  - R4 Physical Access Controls: (Formerly Requirement R2) Changes enumeration of subrequirements to bulleted list.
  - R5 Monitoring Physical Access: (Formerly Requirement R3) Changes enumeration of subrequirements to bulleted list. Changes references to other requirements as appropriate.
  - R6 Logging Physical Access: (Formerly Requirement R4) Changes enumeration of subrequirements to bulleted list. Changes references to other requirements as appropriate.
  - R7 (Formerly Requirement R5)
  - R8 Maintenance and Testing: (Formerly Requirement R6) Changes references to other requirements as appropriate.

- As directed in Order No. 706:
  - R1.7 Updates to the Physical Security Plan: Shortens the time for updates to the Physical Security Plan to 30 calendar days rather than 90 days and adds the word "completion" to the requirement.
  - R1 Physical Security Plan: Changes the term "a senior manager" to "the senior manager."

- Requirements Added:
  - R2 Protection of Physical Access Control Systems: Moves requirement to protect Physical Access Control Systems out of Requirement R1 into its own requirement and excludes hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers from the requirement.
  - R2.1 Protection of Physical Access Control Systems: Adds a requirement that Physical Access Control Systems be protected from unauthorized access.
  - R3 Protection of Electronic Access Control Systems: Adds that cyber assets used in access control and/or monitoring of the Electronic Security Perimeter shall reside within an identified Physical Security Perimeter.

<u>CIP-007-2 Systems Security Management</u>

- As directed in Order No. 706:
  - R2.3 Ports and Services: Removal of the term "or an acceptance of risk."
  - R3.2 Security Patch Mgt.: Removal of the term "or an acceptance of risk."
  - R4.1 Malicious Software Prevention: Removal of the term "or an acceptance of risk."

- R9 Documentation Review and Maintenance: Shortens the time frame to update documentation in response to a system or control change from 90 to 30 calendar days and further clarifies this timeframe to begin after such change is complete.

- Clarifications to ensure that requirements must be implemented:
  - R2 Ports and Services: Explicitly requires the implementation of a process to ensure only required ports and services are enabled.
  - R3 Security Patch Mgt.: Explicitly requires the implementation of Security Patch Management program.
  - R7 Disposal and Redeployment: Explicitly requires the implementation of Cyber Asset disposal and redeployment procedures.

CIP-008-2 Incident Reporting and Response Planning

- As directed in Order No. 706:
  - R1.4 Updating the Cyber Security Incident Response Plan: Shortens the timeframe to update the Incident Response Plan from 90 to 30 calendar days.
  - R1.6 Testing of the Incident Response Plan: Adds language to clarify that testing need not require a responsible entity to remove any systems from service.

- Clarifications to ensure that requirements must be implemented.

- R1 Incident Response Plan: Explicitly requires implementation.

CIP-009-2 Recovery Plans for Critical Cyber Assets

- As directed in Order No. 706:
  - R3 Change Control: Shortens the timeframe for communicating updates to Critical Cyber Asset recovery plans from within 90 to within 30 calendar days of the change being completed.

Implementation Plan for CIP-002-2 through CIP-009-2

- When these standards become effective, the Responsible Entities identified in the Applicability section of the Standard must comply with the requirements. These include:
  - Reliability Coordinator
  - Balancing Authority
  - Interchange Authority
  - Transmission Service Provider

- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

- The Implementation Plan proposes an effective date for the Version 2 CIP Reliability Standards as the first day of the third calendar quarter (*i.e.*, a minimum of two full calendar quarters and not more than three calendar quarters) after Commission approval. Additionally, the Implementation Plan provides that newly registered *entities* must comply with the requirements of the Version 2 CIP Reliability Standards within 24 months of registration. The sole exception is CIP-003-2 Requirement R2, where the newly registered entity must comply within 12 months of registration.
- Furthermore, NERC's Implementation Plan addresses newly *identified* Critical Cyber Assets based on whether or not the entity has an active CIP program. The plan provides an implementation schedule with "compliant" milestones for each CIP Reliability Standard. All timelines are specified as an offset from the date when the Critical Cyber Asset was newly identified.

1. Summary of Stakeholder Comments

The comments raised a variety of issues from minor text edits to compliance concerns, and the SDT prepared a written response to each set of comments received. Some of the more contentious comments centered around the appointment of one senior manager with authority to approve an entity's filing regarding these standards, as well as the latitude regarding the delegation of the senior manager's responsibilities to others.

Concerns were also raised regarding the data retention requirements, the confidentiality of the data retained over extended periods of time, the acceptance of risk, and the removal of the "reasonable business judgment" language. The SDT identified and considered several arguments asserted by stakeholders during the initial ballot of the Version 2 CIP Reliability Standards both for and against approving the proposed CIP Reliability Standards, which are summarized below.

i. Designation of a Single Senior Manager

The designation of a single senior manager, as required by the Commission in its discussion of Reliability Standard CIP-003-1 R2 in Order No. 706 was considered to be overly prescriptive. Entities objected to this requirement by arguing that the standards would prescribe their corporate governance. To a lesser extent, some entities stated that they would prefer to see the senior manager requirement moved to Reliability Standard CIP-002-2.

In response, the SDT stated that the directive in FERC Order No. 706 appropriately justified the revision to the existing standard requirement. The requirement as stated in the standard does not dictate the management structure of the Responsible Entity. The requirement calls for each Responsible Entity to identify a single point of accountability for the implementation and compliance with the CIP Reliability Standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals.

Because Reliability Standard CIP-003-2 is the governance standard of the CIP Reliability Standards and assignment of a Senior Manager is a governance issue, the SDT

chose to leave this requirement in the standard and make Reliability Standard CIP-003-2, Requirement R2 applicable to all Responsible Entities. The SDT plans to revisit the placement of the requirement in a future revision to the standards.

ii. Addition to R1.6 of CIP-006 of "Continuous" to the Escorted Access Requirement

Entities objected to the addition of the word "continuous" to R1.6 of Reliability Standard CIP-006-2 with respect to escorted access. The greatest concern from entities had to do with a perceived inability to enforce and audit compliance with this requirement.

In response to these concerns, the SDT stated that the term "continuous" does not change the original intent or the ability to audit the requirement. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. In response to concerns raised regarding how to demonstrate compliance, the SDT noted that there are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).[14]

iii. Technical Feasibility Exception ("TFE") Process

Entities commented that the TFE process, as the alternative to "Reasonable Business Judgment" language, should have been made available in the standard and not moved to the Uniform Compliance Monitoring and Evaluation Program ("CMEP") in the NERC Rules of Procedure. The concerns raised included the need to define the TFE process in the standards themselves, and the TFE stipulation that the standard must

[14] *See* item # 34 in the Record of Development, included in Exhibit B.

provide for feasibility or the TFE process will not allow the Entity to seek relief. Concerns were also raised with respect to the removal of the assertion in Section D 1.4.2 (Additional Compliance Information) of the NERC Rules of Procedure that duly authorized exceptions would not result in non-compliance.

In response to these concerns, the SDT provided that it has no authority over the approval process for changes to the NERC Rules of Procedure, noting the industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees and will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommended that the industry take advantage of every opportunity to influence the TFE development process. The SDT also stated that an exception against the Responsible Entity's compliance policy does not relieve the Entity from compliance with a requirement of the standard, and therefore, the SDT asserted, a properly approved exception to the Responsible Entity's security policy will not result in non-compliance. Because the exception against a company policy is a separate issue from an exception against the requirement of the standard, a Responsible Entity may find it has to process both types of exceptions.

iv. Modification to Documentation Update Timeframe Requirements

A number of modifications were made to the documentation update timeframe requirements in the Standards--that is, shortening the time from 90 to 30 days. Entities objected to the 30-day timeframe, commenting that the required 30-day timeframe is unrealistic to adequately document and communicate the related changes to all appropriate staff across a company.

In response, the SDT reduced the timeframe for certain documentation requirements to 30 days to conform to applicable directives in FERC Order No. 706. For consistency in the standards, the SDT reduced the documentation update timeframe to 30 days for the remaining standards requirements that were not directly referenced in the FERC Order. The SDT also clarified that the 30-day timeframe begins with the completion of the related change. The SDT noted that the 30-day timeframe for updating documentation is appropriate and reasonable.

A number of additional comments provided during the balloting process included concerns with requirements that were not revised in Phase 1 of the development of Version 2 of the CIP Reliability Standards. These comments were deferred by the SDT with a recommendation to resubmit the comments in future SDT revisions to the CIP Reliability Standards, as appropriate.

V. JUSTIFICATION FOR APPROVAL OF PROPOSED CIP RELIABILITY STANDARDS

As the Commission noted in Order No. 706, the CIP Reliability Standards, together, provide baseline requirements for the protection of critical cyber assets that support an important reliability goal for the nation's bulk Power system.[15] The CIP Reliability Standards provide a comprehensive set of requirements to protect the bulk power system from malicious cyber attacks by requiring bulk power system users, owners and operators to establish a risk-based vulnerability assessment methodology to identify and prioritize critical assets and critical cyber assets. The Version 2 CIP Reliability Standards proposed herein for Commission approval, support these reliability goals and directly address concerns identified by the Commission in Order No. 706.

[15] Order No. 706 at P 24.

Additionally, the Version 2 CIP Reliability Standards strengthen the Cyber Security framework for the identification and protection of bulk power system Critical Assets and Critical Cyber Assets to support reliable operation of the bulk power system. These Version 2 CIP Reliability Standards recognize the differing roles of each entity in the operation of the bulk power system, the criticality and vulnerability of the assets needed to manage bulk power system reliability, and the risks to which they are exposed. Because business and operational demands for managing and maintaining a reliable bulk power system increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other across functions and organizations for services and data, increased risks to these Cyber Assets could result. Accordingly, NERC requests approval of the Version 2 CIP Reliability Standards to help strengthen the security of the bulk power system.

NERC believes Commission approval of the proposed modifications to the CIP Reliability Standards is consistent with the Commission's directives provided in Order No. 706. While further consideration and completion of phased work within the framework of the Reliability Standards Development Process to address the full scope of directives in Order No. 706 is continuing, in the near-term, NERC believes that timely approval of the changes proposed in this petition are necessary to maintain and strengthen the reliability and security of the bulk power system.

VI. CONCLUSION

For the reasons discussed above, NERC believes that the best interest of reliability is served through the approval of the proposed Version 2 CIP Reliability Standards. The key reliability objective of these Reliability Standards is maintained from the original Version 1 of the CIP Reliability Standards as the proposed modifications discussed in this filing support and further those objectives by addressing some of the Commission's concerns in Order No. 706.

Accordingly, NERC respectfully requests that the Commission approve the Version 2 CIP Reliability Standards and make them effective in accordance with the effective date provisions set forth in the proposed Reliability Standards, along with the accompanying implementation plans. Additionally, NERC is not requesting approval for revised VRFs or VSLs associated with the Version 2 CIP Reliability Standards with this filing, but will request approval of revised VRFs and VSLs that will be submitted in a filing to the Commission no later than December 21, 2009.

Respectfully submitted,

Rick Sergel
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney
Rebecca J. Michael
Assistant General Counsel
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
rebecca.michael@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 22nd day of May, 2009.

/s/ Holly A. Hawkins
Holly A. Hawkins

Assistant General Counsel for North American Electric Reliability Corporation

Exhibit A

Reliability Standards Proposed for Approval

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

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

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

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

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-2

3. Purpose: Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g. emails, memos, computer based training, etc.);
- Indirect communications (e.g. posters, intranet, brochures, etc.);

- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program**.** Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

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

2. Number: CIP-005-2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity.	

		Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-2

3. Purpose: Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-006-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-2

3. Purpose: Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-2

3. Purpose: Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	

Exhibit B

Record of Development of Proposed Reliability Standards

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)
Exhibit B – Index for the Record of Development of Proposed Reliability Standards CIP-002-2 through CIP-009-2

Cyber Security (Project 2008-06)

Registered Ballot Body | Related Files | Drafting Team Rosters

All Critical Infrastructure Protection Standards Activities

Status — VRFs and VSLs
The Cyber Security Standard Drafting Team has posted its Version 2 Violation Severity Levels for CIP-002-2 through CIP-009-2 and the Violation Risk Factors for CIP-003-2 and CIP-006-2.

Status — Draft Standards
The ballot pool approved the standards revisions. The revised standards will be submitted to the NERC Board of Trustees for adoption.

Purpose / Industry Need
This set of revisions in this project includes:

- Modifying the standards so they conform to the latest approved versions of the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1.
- Addressing the directives issued by FERC, in Order 706 relative to the approved Cyber Security Standards CIP-002-1 through CIP-009-1. Refer to http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf the complete text of the final order. Specific requirements from the Order are identified in Attachment 2.
  – Emphasis on Order 706 directive for NERC to address revisions to the CIP standards considering applicable feature of the NIST Security Risk Management Framework among other resources.
- Incorporating clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

NOTE: Additional issues identified by stakeholders during the posting of this SAR are listed in a supplementary SAR. The supplementary SAR will be posted for industry comment, and if supported by stakeholders, will be appended to this SAR.

Proposed Standard	Supporting Materials	Comment Period	Comments Received	Response to Comments
Announcement **(35)** Second Draft of Revised Cyber Security Standards CIP-002-2 through CIP-009-2 Posted for a 10-day Recirculation Ballot Window Clean and Redline Versions to last posting (zip file) **(Same as #24)** Redline Versions to last approval (zip file) **(Same as #25)**	Version 2 Implementation Plan clean **(Same as #26)** | redline **(Same as #27)** to last posting Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities clean **(Same as #28)** | redline **(Same as #29)** to last posting	04/17/09 - 04/27/09 (closed) **Recirculation Ballot**		Announcement **(36)** Ballot Results **(37)**
Announcement **(30)** Second Draft of Revised Cyber Security Standards CIP-002-2 through CIP-009-2 Posted for a 10-day Ballot Window Clean and Redline Versions to last posting (zip file) **(Same as #24)** Redline Versions to last approval (zip file) **(Same as #25)**	Version 2 Implementation Plan clean **(Same as #26)** | redline **(Same as #27)** to last posting Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities clean **(Same as #28)** | redline **(Same as #29)** to last posting	04/01/09 - 04/10/09 (closed) **Ballot**		Announcement **(31)** Ballot Results **(32)** Additional Ballot Comments **(33)** Consideration of Comment **(34)**
Announcement Version 2 VSLs for CIP-002-2 through CIP-009-2 and Version 2 VRFs for CIP-003-2 and CIP-006-2 Version 2 Violation Severity Levels (for CIP-002-2 through CIP-009-2)	Complete set of materials for commenting on Project 2008-06 and Project 2008-14 (zip)	03/16/09 - 04/20/09 (closed) Comment Form *Please submit only one comment form. The form covers Project 2008-06 and Project 2008-14.	Comments Received	

Proposed Standard	Supporting Materials	Comment Period	Comments Received	Response to Comments
Version 2 Violation Risk Factors (for CIP-003-2 and CIP-006-2)				
Announcement **(23)** Second Draft of Revised Cyber Security Standards CIP-002-2 through CIP-009-2 Posted for a 30-day Pre-ballot Review Clean and Redline Versions to last posting (zip file) **(24)** Redline Versions to last approval (zip file) **(25)**	Version 2 Implementation Plan clean **(26)** | redline **(27)** to last posting Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities clean **(28)** | redline **(29)** to last posting	03/03/09 - 04/01/09 (closed) Join Ballot Pool		
Announcement **(16)** First Draft of Revised Cyber Security Standards CIP-002-1 through CIP-009-1 Posted for 45-day Comment Period CIP-002-1 through CIP-009-1 Clean and Redline Versions **(17)** (zip file)	Implementation Plan **(18)** Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities **(19)**	11/21/08 – 01/05/09 Electronic Comment Form Word Version **(20)**	Comments Received **(21)** (Please select icon in the left hand column to see individual response.)	Consideration of Comments **(22)**
		Announcement **(14)** 07/15/08 - 07/28/08 (closed) Electronic Nomination Form Nomination Form (Word version) **(15)**		

Proposed Standard	Supporting Materials	Comment Period	Comments Received	Response to Comments
Draft SAR Version 2 Cyber Security Standards Draft SAR Version 2 Clean **(9)** | Redline **(10)** Attachment 2 — Excerpts from FERC Order 706 **(11)** Cyber Standards — Last approved **(12)**	Letter from NERC President and CEO on Cyber Security **(13)**			
Announcement **(3)** Draft SAR Version 1 Cyber Security Standards Posted for 30-day Comment Period Draft SAR Version 1 **(4)** Cyber Standards — Last approved **(5)**		03/20/08 – 04/19/08 (closed) Comment Form Questions **(6)** Announcement **(1)** 03/20/08 – 04/04/08 (closed) Nomination Form **(2)**	Comments **(7)**	Consideration of Comments **(8)**
To download a file click on the file using your right mouse button, then save it to your computer in a directory of your choice.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Nomination Period Opens for SAR Drafting Team
March 20–April 4, 2008

Now available at: http://www.nerc.com/~filez/standards/Project_2008-06_Cyber_Security.html

The Standards Committee is seeking industry experts to serve on the Cyber Security SAR Drafting Team. This project involves making revisions to the following standards to address FERC's directives in Order 706 and to bring the set of standards into conformance with the ERO Rules of Procedure:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

If you are interested in serving on this team, please complete this nomination form no later than April 4, 2008.

Standards Development Procedure

The *Reliability Standards Development Procedure Manual* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Maureen Long, Standards Process Manager, at maureen.long@nerc.net or at (813) 468-5998.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Nomination Form for Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

Please return this form to sarcomm@nerc.net by **April 4, 2008** with the words "Cyber Security Standard Drafting Team" in the subject line. If you have any questions, please contact David Taylor at David.Taylor@nerc.net or by telephone at 609-452-8060.

All candidates should be prepared to participate actively at these meetings.

Name: Organization: Address: Office Telephone: E-mail:
Please briefly describe your experience and qualifications for participating on the standard drafting team for Project 2008-06 Cyber Security Oder 706. Please provide details of your experience, as applicable, related to: • developing or implementing cyber security policies and procedures, • implementing or managing the implementation of the cyber security standards, • implementing substation automation, protection and control, or plant or boiler control systems (this field experience does not need to be security related – it will be used to augment the viewpoints of the drafting team to provide more realistic and practical modifications to the standards) • previous experience working on or applying NIST standards • experience writing compliance elements in support of NERC standards. NERC staff will use the information provided as the basis for developing a recommendation to the Standards Committee for the standard drafting team for Project 2008-06 Cyber Security Oder 706. It is very important that the information you provide be concise and clearly indicate why you feel you are qualified to participate on this team.

I represent the following NERC	**I represent the following Industry Segment (check one):**

Reliability Region(s) (check all that apply):		
☐ ERCOT ☐ FRCC ☐ MRO ☐ NPCC ☐ RFC ☐ SERC ☐ SPP ☐ WECC ☐ NA – Not Applicable	☐	1 — Transmission Owners
	☐	2 — RTOs, ISOs
	☐	3 — Load-serving Entities
	☐	4 — Transmission-dependent Utilities
	☐	5 — Electric Generators
	☐	6 — Electricity Brokers, Aggregators, and Marketers
	☐	7 — Large Electricity End Users
	☐	8 — Small Electricity End Users
	☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities

Which of the following Function(s)[1] do you have expertise or responsibilities:

☐ Balancing Authority	☐ Planning Coordinator
☐ Compliance Monitor	☐ Transmission Operator
☐ Distribution Provider	☐ Transmission Owner
☐ Generator Operator	☐ Transmission Planner
☐ Generator Owner	☐ Transmission Service Provider
☐ Interchange Authority	☐ Purchasing-selling Entity
☐ Load-serving Entity	☐ Resource Planner
☐ Market Operator	☐ Reliability Coordinator

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group.

Name:	Office Telephone:
Organization:	E-mail:
Name:	Office Telephone:
Organization:	E-mail:

[1] These functions are defined in the NERC Functional Model, which is downloadable from the NERC Web site.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Corrected Links to Cyber Security Web Page Standards Announcement

Comment Periods Open
March 20, 2008–April 19, 2008 (Cyber Security SAR)
March 20, 2008–May 3, 2008 (Relay Loadability Reference Document)

Now available at: http://www.nerc.com/~filez/standards/Project_2008-06_Cyber_Security.html

Comment Period for Project 2008-06 — Cyber Security SAR Opens March 20, 2008

This SAR for Project 2008-06 — Cyber Security has been posted for a 30-day comment period through April 19, 2008.

The SAR proposes modifications to bring the following standards into conformance with the ERO Rules of Procedure and to address the directives from FERC Order 706:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Please use this electronic comment form to submit comments on this SAR.

If you need an off-line, unofficial copy of the questions in the comment form, there is a copy posted at the following Web site:

http://www.nerc.com/~filez/standards/Project_2008-06_Cyber_Security.html

Please use only the electronic comment form to submit comments on the SAR for Cyber Security by April 19, 2008. If you experience any difficulties in using the electronic form, please contact Barbara Bogenrief at 609-452-8060.

Now available at: http://www.nerc.com/~filez/standards/Relay-Loadability.html

Comment Period for Relay Loadability Reference Document Opens March 20, 2008

A reference document titled "Determination and Application of Practical Relaying Loadability Ratings" has been posted for a 45-day comment period through May 3, 2008.

The purpose of this reference document is to aid entities in understanding the requirements within PRC-023-1. This reference document is not intended to present additional requirements and should not be construed to do so, even though some of the text may appear to be prescriptive. In accordance with the *Reliability Standards Development Procedure*, reference documents may explain or facilitate implementation of a standard but do not contain mandatory requirements subject to compliance review.

Please use this electronic comment form to submit comments on the Transmission Relay Loadability reference document.

If you need an off-line, unofficial copy of the questions in the comment form, there is a copy of the comment form posted at the following site:

http://www.nerc.com/~filez/standards/Relay-Loadability.html

Please use only the electronic comment form to submit comments on the Transmission Relay Loadability reference document by May 3, 2008. If you experience any difficulties in using the electronic form, please contact Barbara Bogenrief at 609-452-8060.

Standards Development Procedure

The *Reliability Standards Development Procedure Manual* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Maureen Long, Standards Process Manager, at maureen.long@nerc.net or at (813) 468-5998.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009)
Request Date March 1, 2008

SAR Requester Information	**SAR Type** (*Check a box for each one that applies.*)	
Name NERC Staff	☐	New Standard
Primary Contact Scott R. Mix	☒	Revision to existing Standards
Telephone 215-853-8204 Fax	☐	Withdrawal of existing Standard
E-mail scott.mix@nerc.net	☐	Urgent Action

Purpose (Describe what the standard action will achieve in support of bulk power system reliability.)

To protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

Implement Changes to the following Cyber Security Standards as indicated in FERC Order 706:

- CIP-002-1 Critical Cyber Asset Identification
- CIP-003-1 Security Management Controls
- CIP-004-1 Personnel & Training
- CIP-005-1 Electronic Security Perimeter(s)
- CIP-006-1 Physical Security of Critical Cyber Assets
- CIP-007-1 Systems Security Management
- CIP-008-1 Incident Reporting and Response Planning
- CIP-009-1 Recovery Plans for Critical Cyber Assets

Brief Description (Provide a paragraph that describes the scope of this standard action.)

This set of revisions will implement the modifications directed by FERC, in their Order 706, to the approved Cyber Security Standards CIP-002-1 through CIP-009-1. Refer to http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf for the complete text of the final order. Specific requirements from the Order will be identified during the SAR and/or Standards Drafting process.

In addition, the drafting team will modify the standards so they conform to the latest approved versions of the Reliability Standards Development Procedure and the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.)

This proposed standards drafting project will address all of the directed modifications identified in the FERC Final Order 706. There are a significant number of directed modifications to the set of cyber security standards. Some of them are of low consequence, and low controversy, while others are more significant changes, with more contentious issues. There may be a third set of changes that are in between these two extremes. Whether there are two or three "classes" of changes will be left to the Standards Drafting Team.

As envisioned, the standard drafting team will address the "low hanging fruit" and rapid turn-around issues first, working on some of the more contentious issues while the less contentious issues are in either comment or ballot mode. This may allow for multiple revisions to the standards where some changes are reviewed by industry, balloted, and submitted for approval during the development and comment cycle of the remaining contentious issues.

The end result of this SAR may be more than one set of revised standards submitted for approval.

This SAR also proposes to add the following from the original Cyber Security Standards SAR finalized on March 8, 2004:

- Regional Entities and Purchasing-Selling Entity functions to the applicability section of the standards.
- Reliability and Market Interface Principle 4 (plans for emergency operation and system restoration).

If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator – see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Regional Entity	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☒	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☒	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Related Standards

Standard No.	Explanation
CIP-001	Sabotage Reporting (no change proposed)
CIP-002	Critical Cyber Asset Identification – FERC directed modifications
CIP-003	Security Management Controls – FERC directed modifications
CIP-004	Personnel and Training – FERC directed modifications
CIP-005	Electronic Security Perimeter – FERC directed modifications
CIP-006	Physical Security – FERC directed modifications
CIP-007	Systems Security Management – FERC directed modifications
CIP-008	Incident Reporting and Response Planning – FERC directed modifications
CIP-009	Recovery Plans – FERC directed modifications

Related SARs

SAR ID	Explanation
None	

Regional Variances

Region	Explanation
ERCOT	None
FRCC	None
MRO	None
NPCC	None
SERC	None
RFC	None
SPP	None
WECC	None

Attachment 1 - Standard Review Guidelines

Technical Basis in Engineering and Operations
Is this reliability standard based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field?

Purpose
Does this reliability standard have a clear statement of purpose that describes how the standard contributes to the reliability of the bulk power system? Each purpose statement should include a value statement.

Applicability
Does this reliability standard clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted? Where multiple functional classes are identified is there a clear line of responsibility for each requirement identifying the functional class and entity to be held accountable for compliance? Does the requirement allow overlapping responsibilities between Registered Entities possibly creating confusion for who is ultimately accountable for compliance?

Does this reliability standard identify the geographic applicability of the standard, such as the entire North American bulk power system, an interconnection, or within a regional entity area? If no geographic limitations are identified, the default is that the standard applies throughout North America.

Does this reliability standard identify any limitations on the applicability of the standard based on electric facility characteristics, such as generators with a nameplate rating of 20 MW or greater, or transmission facilities energized at 200 kV or greater or some other criteria? If no functional entity limitations are identified, the default is that the standard applies to all identified functional entities.

If the applicability is to a set of responsible entities that have criteria other than the criteria used in the compliance registration process, then the applicability section of the standard should include the reliability-related reason for the unique applicability criteria.

Effective Dates
Must be 1st day of 1st quarter after entities are expected to be compliant – must include time to file with regulatory authorities and provide notice to responsible entities of the obligation to comply. If the standard is to be actively monitored, time for the Compliance Monitoring and Enforcement Program to develop reporting instructions and modify the Compliance Data Management System(s) both at NERC and Regional Entities must be provided in the implementation plan. The effective date should be linked to the applicable regulatory approvals – here is the default sentence to use for standards that should become effective as soon as possible:

First day of first calendar quarter after applicable regulatory approval (or, in those jurisdictions where regulatory approval is not required, the standard becomes effective on the first day of the first calendar quarter after BOT adoption.)

Performance Requirements
Does this reliability standard state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest?

Does each requirement identify who shall do what under what conditions and to what outcome?

Fill-in-the-blank Requirements
Do not include any 'fill-in-the-blank' requirements. These are requirements that assign one entity responsibility for developing some performance measures without requiring that the performance measures be included in the body of a standard – then require another entity to comply with those requirements.

Every reliability objective can be met, at least at a threshold level, by a North American standard. If we need regions to develop regional standards, such as in under-frequency load shedding, we can always write a uniform North American standard for the applicable functional entities as a means of encouraging development of the regional standards.

Requirements for Regional Reliability Organization
Do not write any requirements for the Regional Reliability Organization. Any requirements currently assigned to the RRO should be re-assigned to the applicable functional entity. If the requirement can only be performed at a regional level, assign the requirement to the Regional Entity, not the RRO.

Violation Risk Factors
Each requirement must have an associated Violation Risk Factor (VRF). Avoid assigning a VRF to sub-requirements. If a sub-requirement needs a VRF that is different from the VRF assigned to the main requirement, then consider sub-dividing the requirement into multiple requirements. The VRF identifies the reliability-related risk of violating a requirement.

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures;

or a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures;

or a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. A requirement that is administrative in nature;

or a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively

monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

Time Horizon
The drafting team should also indicate the time horizon available for mitigating a violation to the requirement using the following definitions:

- **Long-term Planning** — a planning horizon of one year or longer.
- **Operations Planning** — operating and resource plans from day-ahead up to and including seasonal.
- **Same-day Operations** — routine actions required within the timeframe of a day, but not real-time.
- **Real-time Operations** — actions required within one hour or less to preserve the reliability of the bulk electric system.
- **Operations Assessment** — follow-up evaluations and reporting of real time operations.

Measurability
Is each performance requirement stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement?

Does each performance requirement have one or more associated measures used to objectively evaluate compliance with the requirement? Measures should comply with the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" reference document.

If performance results can be practically measured quantitatively, are metrics provided within the requirement to indicate satisfactory performance?

Violation Severity Levels
The drafting team should indicate a set of violation severity levels that can be applied for the requirements within a standard. ('Violation severity levels' replace existing 'levels of non-compliance.') The violation severity levels must be applied for each requirement and may be combined to cover multiple requirements, as long as it is clear which requirements are included and that all requirements are included.

The violation severity levels should be based on the following definitions and the latest version of the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards":

- **Lower: mostly compliant with minor exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more minor details.
- **Moderate: mostly compliant with significant exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more significant elements.
- **High: marginal performance or results** — The responsible entity has only partially achieved the reliability objective of the requirement and is missing one or more significant elements.
- **Severe: poor performance or results** — The responsible entity has failed to meet the reliability objective of the requirement.

Compliance Enforcement Authority
Replace, 'Regional Reliability Organization' with 'Regional Entity'

Replace, 'NERC' with 'ERO'
In situations where the Regional Entity is the responsible entity, or where a responsible entity works for the Regional Entity, the Compliance Enforcement Authority is the ERO. In all other situations, the Regional Entity is the Compliance Enforcement Authority.

Compliance Monitoring Period and Reset Timeframe
In all cases, enter, 'Not applicable.' (These terms are associated with an older version of the sanctions table. The next time the Reliability Standards Development Procedure is updated, the procedure will be revised to omit references to 'compliance monitoring period' and 'reset timeframe'.)

Data Retention
Use the data retention periods proposed in the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" document unless there is a justifiable reason for proposing other data retention periods.

Compliance Monitoring Processes
The list of compliance monitoring processes used with each standard should comply with the proposed list of processes identified in the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" reference document. In the standard, list the compliance monitoring processes under 'Additional Compliance Information.'

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Periodic Data Submittals
- Exception Reporting
- Complaints

Associated Documents
We will delay populating this section of the standard with a list of 'related' standards because standards are all being changed and many will have new numbers. We should limit the references to those support documents that are useful in complying with the standard.

Functional Model Version 3
Review the requirements against the latest descriptions of the responsibilities and tasks assigned to functional entities as provided in pages 13 through 53 of the draft Functional Model Version 3.

Completeness
Is this reliability standard complete and self-contained? Does the standard depend on external information to determine the required level of performance?

Clear Language
Is the reliability standard stated using clear and unambiguous language? Can responsible entities, using reasonable judgment and in keeping with good utility practices, arrive at a consistent interpretation of the required performance?

Consistent Terminology
To the extent possible, does this reliability standard use a set of standard terms and definitions that are approved through the NERC reliability standards development process?

If the standard uses terms that are included in the NERC Glossary of Terms Used in Reliability Standards, then the term must be capitalized when it is used in the standard. New terms should not be added unless

they have a ‘unique’ definition when used in a NERC reliability standard. Common terms that could be found in a college dictionary should not be defined and added to the NERC Glossary.

Practicality
Does this reliability standard establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter?

Consequences for Noncompliance
In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, are the consequences of violating a standard clearly known to the responsible entities?

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-1

3. Purpose: NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

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

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:

M1. The risk-based assessment methodology documentation as specified in Requirement R1.

M2. The list of Critical Assets as specified in Requirement R2.

M3. The list of Critical Cyber Assets as specified in Requirement R3.

M4. The records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002 from the previous full calendar year

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1 Level 1: The risk assessment has not been performed annually.

2.2 Level 2: The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.

2.3 Level 3: The list of Critical Assets or Critical Cyber Assets does not exist.

2.4 Level 4: The lists of Critical Assets and Critical Cyber Assets do not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change “Control Center” to “control center”	03/24/06

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-1

3. Purpose: Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-003, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-003:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

R2.1. The senior manager shall be identified by name, title, business phone, business address, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

M1. Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.

M3. Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.

M4. Documentation of the Responsible Entity's information protection program as specified in Requirement R4.

M5. The access control documentation as specified in Requirement R5.

M6. The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,

2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,

2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,

2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,

2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

2.4.1 No cyber security policy exists; or,

2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,

2.4.3 No documented change control and configuration management process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-1

3. Purpose: Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-004, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-004:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-004:

R1. Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

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

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:

M1. Documentation of the Responsible Entity's security awareness and reinforcement program as specified in Requirement R1.

M2. Documentation of the Responsible Entity's cyber security training program, review, and records as specified in Requirement R2.

M3. Documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. Documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.3.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,

2.1.2 Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,

2.1.3 Personnel risk assessment program exists, but documentation of that program does not exist; or,

2.1.4 List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.

2.1.5 One personnel risk assessment is not updated at least every seven years, or for cause; or,

2.1.6 One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.

2.2. Level 2:

2.2.1 Awareness program does not exist or is not implemented; or,

2.2.2 Training program exists, but does not address the requirements identified in Standard CIP-004; or,

2.2.3 Personnel risk assessment program exists, but assessments are not conducted as required; or,

2.2.4 One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.

2.3. Level 3:

2.3.1 Training program exists, but has not been reviewed and updated at least annually; or,

2.3.2 A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,

2.3.3 List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.

2.4. Level 4:

2.4.1 No documented training program exists; or,

2.4.2 No documented personnel risk assessment program exists; or,

2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel termination for cause…”	03/24/06
1	06/01/06	D.2.1.4 — Change “access control rights” to “access rights.”	06/05/06

A. Introduction

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

2. Number: CIP-005-1

3. Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability

4.1. Within the text of Standard CIP-005, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-005:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; and,

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

M1. Documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's annual vulnerability assessment as specified in Requirement R4.

M5. Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,

2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,

2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-1

3. Purpose: Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-006, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-006:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

R2. Physical Access Controls **—** The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms

for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

R5. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:

R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.

R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the review and updating of the plan.

M2. Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.

M3. Documentation identifying the methods for monitoring physical access as specified in Requirement R3.

M4. Documentation identifying the methods for logging physical access as specified in Requirement R4.

M5. Access logs as specified in Requirement R5.

M6. Documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documents other than those specified in Requirements R5 and R6.2 from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,

2.1.2 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.1.3 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

2.1.4 Physical access logs are retained for a period shorter than ninety days; or,

2.1.5 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

2.1.6 One required document does not exist.

2.2. Level 2:

2.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

2.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

2.2.4 More than one required document does not exist.

2.3. Level 3:

2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,

2.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

2.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.4.3 No maintenance or testing program exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-1

3. Purpose: Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-007, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-007:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

M1. Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.

M2. Documentation as specified in Requirement R2.

M3. Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.

M4. Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.

M5. Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.

M6. Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.

M7. Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. Documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or

2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,

2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
- Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

2.2. Level 2:

2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,

2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.3. Level 3:

2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,

2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4. Level 4:

2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,

2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4.3 No logs exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-1

3. Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability

4.1. Within the text of Standard CIP-008, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-008:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-008:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all

reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of CIP-008:

M1. The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan

M2. All documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.4.4 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Levels of Noncompliance

2.1. Level 1: A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.

2.2. Level 2:

2.2.1 A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,

2.2.2 A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,

2.2.3 Records related to reportable Cyber Security Incidents were not retained for three calendar years.

2.3. Level 3:

2.3.1 A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,

2.3.2 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.

2.4. Level 4: A Cyber Security Incident response plan does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-1

3. Purpose: Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-009, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Reliability Organizations

4.2. The following are exempt from Standard CIP-009:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-009:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:

M1. Recovery plan(s) as specified in Requirement R1.

M2. Records documenting required exercises as specified in Requirement R2.

M3. Documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. Documentation regarding backup and storage of information as specified in Requirement R4.

M5. Documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-009 from the previous full calendar year.

1.3.2 The Compliance Monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,

2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.

2.2. Level 2:

2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,

2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.

2.3. Level 3:

2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,

2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.

2.4. Level 4:

2.4.1 No recovery plan(s) exist; or,

2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Comment Form — Project 2008-06 Questions

Background Information:

In Order 706 FERC directed that NERC make significant changes to each of the following Cyber Security standards:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

A SAR to revise each of these standards has been posted for stakeholder review. The scope of the SAR includes addressing the directives in Order 706. Refer to http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf for the complete text of the final order.

The SAR proposes expanding the scope of applicable entities to include the Regional Entity and Purchasing-selling Entity. If the Functional Model Work Group implements changes to the Functional Model in response to Order 706 (i.e., Demand Side Aggregator – see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR.

In addition, the scope of the SAR includes making revisions to the standards so they conform to the latest approved versions of the Reliability Standards Development Procedure and the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1 of the SAR.

While the SAR is still under development, stakeholders can identify additional improvements needed in this set of standards.

Please review the SAR and then answer the following questions. Please submit your responses no later than **April 19, 2008**.

If you experience any problems in using this form, please contact Barbara Bogenrief at 609-452-8060.

Questions:

1. Do you agree with the scope of the proposed standards action?

   ☐ Yes

   ☐ No

   Comments:

2. This SAR proposes to add the Regional Entities and Purchasing-Selling Entity functions to the applicability section of the revised standards. If additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria) as a direct result of Order 706 (i.e., Demand Side Aggregator — see Order 706 paragraph 51), which directly impact the applicable functions, conforming modifications will be made to the cyber security standards.

   Do you agree with these proposed changes to the applicability sections of these standards?

   ☐ Yes

   ☐ No

   Comments:

3. If you are aware of any regional variances or associated business practices that we should consider with this SAR please identify them here

   Regional Variance:

   Business Practice:

4. Do you agree with the "multi-phase" approach identified in the SAR? (The SAR's proposal is to take the easiest modifications through the posting and balloting cycles first, followed by one or more sets of modifications to address those directives that will take more time.)

   ☐ Yes

   ☐ No

   Comments:

5. Based on the limited experience of implementing the current standards, are there any other issues that are not addressed in Order 706 that should be changed?

   ☐ Yes

   ☐ No

   Comments:

6. If you have any other comments on this SAR that you haven't already provided in response to the prior six questions, please provide them here.

   Comments:

Comments — Project 2008-06

Background Information:

In Order 706 FERC directed that NERC make significant changes to each of the following Cyber Security standards:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

A SAR to revise each of these standards has been posted for stakeholder review. The scope of the SAR includes addressing the directives in Order 706. Refer to http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf for the complete text of the final order.

The SAR proposes expanding the scope of applicable entities to include the Regional Entity and Purchasing-selling Entity. If the Functional Model Work Group implements changes to the Functional Model in response to Order 706 (i.e., Demand Side Aggregator – see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR.

In addition, the scope of the SAR includes making revisions to the standards so they conform to the latest approved versions of the Reliability Standards Development Procedure and the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1 of the SAR.

While the SAR is still under development, stakeholders can identify additional improvements needed in this set of standards.

Please review the SAR and then answer the following questions. Please submit your responses no later than **April 19, 2008**.

If you experience any problems in using this form, please contact Barbara Bogenrief at 609-452-8060.

Questions:

1. Do you agree with the scope of the proposed standards action?

   ☐ Yes

   ☐ No

   Comments:

2. This SAR proposes to add the Regional Entities and Purchasing-Selling Entity functions to the applicability section of the revised standards. If additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria) as a direct result of Order 706 (i.e., Demand Side Aggregator — see Order 706 paragraph 51), which directly impact the applicable functions, conforming modifications will be made to the cyber security standards.

   Do you agree with these proposed changes to the applicability sections of these standards?

   ☐ Yes

   ☐ No

   Comments:

3. If you are aware of any regional variances or associated business practices that we should consider with this SAR please identify them here

   Regional Variance:

   Business Practice:

4. Do you agree with the "multi-phase" approach identified in the SAR? (The SAR's proposal is to take the easiest modifications through the posting and balloting cycles first, followed by one or more sets of modifications to address those directives that will take more time.)

   ☐ Yes

   ☐ No

   Comments:

5. Based on the limited experience of implementing the current standards, are there any other issues that are not addressed in Order 706 that should be changed?

   ☐ Yes

   ☐ No

   Comments:

6. If you have any other comments on this SAR that you haven't already provided in response to the prior six questions, please provide them here.

Individual
Terri Eaton
Xcel Energy
303-273-4878
terri.k.eaton@xcelenergy.com
MRO, SPP, WECC
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
No
PSEs are involved in scheduling purchase and sales transactions between entities in the wholesale electric market. We are not aware of any activities undertaken by a PSE that could be manipulated from a cyber standpoint and result in compromising the integrity of the bulk electric system. We believe that NERC should be required to provide a credible justification for extending the reach of the CIP standards to PSEs. At this juncture, Xcel Energy does not believe that any such justification has been provided.
No
As noted above, we do not believe that any justification has been provided for extending the reach of the CIP standards to PSEs.
As noted above, the rationale for applying the CIP standards to PSEs has not been provided. Absent an understanding of the reasons for pulling PSEs within the ambit of the CIP standards, we are unable to comment on the need for any regional or business practice variance.
As noted above, the rationale for applying the CIP standards to PSEs has not been provided. Absent an understanding of the reasons for pulling PSEs within the ambit of the CIP standards, we are unable to comment on the need for any regional or business practice variance.
No
Any further changes to the CIP standards should be proposed and adopted on a comprehensive basis. The piecemeal approach contemplated in this question creates a significant risk that changes adopted in one cycle could be altered or overridden by changes approved in a subsequent cycle, undermining the ability of stakeholders to efficiently and effectively manage costs of implementing the CIP standards. The industry is engaged in a very substantial effort to ramp up to comply with the existing standards. This effort will result in substantial additional costs to companies and consumers. While this effort is ongoing, the CIP landscape is continuing to change, creating the very real possibility that work that is currently ongoing will become obsolete with the next round of CIP standards. The current situation will only be exacerbated if the next phase of the CIP standards are adopted on a piecemeal basis.
Yes
First, we believe that a shift in the approach to development of the CIP standards is needed. We believe that the standards need to be redirected toward performance-based expectations rather than command and control directives. The command and control approach currently embodied in the standards is too rigid and inflexible in a rapidly changing environment to effectively and efficiently protect grid assets from cyber threats that may develop in the coming years. A more performance-based approach would allow industry the flexibility to adjust to a rapidly changing environment in the most efficient and effective manner. In addition, an overall goal or mission statement for the CIP process should be established that clearly identifies the objectives of the standards. Presently, we believe that the distinction between cyber security (which we understand to be the objective of the standards) and physical security is not being effectively maintained in the standards. Clarity about the objective of the CIP standards should help ensure a more clear and precise set of changes to the standards.
It is not clear that the current body of CIP standards was based on any real assesment or understanding of potential risks to the bulk electric system of terroristic threats. Rather, it appears that the standards were developed at the micro level based on perceived risks to specific pieces of equipment without a holistic understanding of how grid systems work or where the greatest vulnerabilities really lie. We believe that the next round of CIP standards should be guided by a more clearly defined set of risks which can result in a more focused and effective set of compliance expectations.
Individual
Todd Thompson
PJM Interconection
(610) 666-8264
thompt@pjm.com
RFC
2 - RTOs and ISOs
Yes

Yes
Regional variances should be few if any. The Regional Entities will need to apply compliance guidelines consistently across the U.S. in order to circumvent issues with inconsistency.
Yes
No
It is vitally important that NERC and the Regional Entities work together to provide a common set of audtiting guidelines so that they may be distributed to the industry to help with compliance efforts. Each Responsible Entity has been left with the task of interpreting the CIP Standard requirements and have no way of telling whether their efforts and opinions are correct. There is a very real and serious concern by the Responsible Entities that they could be found in non-compliance due to a difference in opinion or interpretation of any given CIP Standard requirement. With an aggressive Implementation Schedule, these concerns should be addressed as soon as possible. After the SAR process is completed, the same guidance will need to be developed and produced to the Responsible Entities in the industry.
Individual
Kent Kujala
Detroit Edison
(313) 235-9428
kujalak@dteenergy.com
RFC
3 - Load-serving Entities, 5 - Electric Generators, 4 - Transmission-dependent Utilities
Yes
Yes
No
A "multi-phase" approach is a sound idea for a task of this magnitude however, the order of modifications should be based on priority rather than ease of implementation. FERC Order 706 clearly stated that "Reasonable Business Judgment" (P138) and "Acceptance of Risk" (P150) need to be removed and "Technical Feasibility" exceptions need to have criteria developed to ensure accountability (P222). The first two would most likely fall into the easy category and the third might not. The "Technical Feasibility" language used by FERC indicates that it should be high on the priority list and should not be delayed because it may be difficult to address. Other high priority issues should include Periodic Self Certifications (P96). The drafting team should consider all of FERC's comments, determine priorities, and plan a revision schedule based on those priorities
No
Group
Ontario Power Generation
Colin Anderson
Ontario Power Generation
5 - Electric Generators
(416) 592-3326
colin.anderson@opg.com
Yes
see comments below
No
I see no need to expand the applicability of the CIP Standards to PSEs. This appears to be an indirect method of including market data - a subject that was contemplated within FERC's NOPR and widely opposed.

No
The multi-phase approach appears cumbersome and confusing. The standards will be in a perpetual state of flux and members will have a more difficult time implementing programs to ensure compliance against a moving target. Modifications should be done in a comprehensive fashion.
No
Individual
Jason Shaver
American Transmission Company
(262) 506-6885
jshaver@atcllc.com
RFC, MRO
1 - Transmission Owners
No
The SAR should be revised to include a list of all FERC issued directives including the identification of any specific due dates. This additional information will help the industry understand the amount of work the standards drafting team is being assigned. NERC likely has this information so the inclusion of the data should be simple.
Yes
ATC is not aware of any regional or business variance that the SDT should consider.
Yes
Including a list of all FERC order directives will aid that industry and the SDT to efficiently organize the multiple phases.
Yes
The SDT should develop a standard timeline for a newly identified Critical Asset to reach compliance. Any newly identified Critical Asset will take a considerable amount of time for an entity to become fully compliant with the CIP Standards (CIP-002 - 009). This is not included in the existing CIP standards but we believe that it is something that should be addressed in the phase of standards development. Also, by including a list of all FERC ordered directives in the SAR that SDT will be able to determine when it's best to address these other suggested changes.
Group
PPL Supply
Annette Bannon
PPL Generation, LLC
5 - Electric Generators, 6 - Electicity Brokers, Aggregators
610-774-2064
ambannon@pplweb.com
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
RFC, RFC
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
MRO, MRO
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus

PPL EnergyPlus
NPCC, NPCC
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
SERC, SERC
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
SPP, SPP
6, 6
Jim Batug
Jim Batug
PPL Generation
PPL Generation
RFC, RFC
5, 5
Jim Batug
Jim Batug
PPL Generation
PPL Generation
NPCC, NPCC
5, 5
Yes
No
PPL Supply disagrees with the intent to add the PSE funtion to the CIP applicability. It is not clear to PPL how the transactions by a PSE would involve critical cyber assets essential to the reliable operations of the BPS.
No
PPL Supply disagrees with the SDT's approach to addressing issues through multiple revisions. This approach will add complexity and rapid changes to the standards making it difficult for entities dealing with implementing plans, some with long lead-times, to be compliant with the changing requirements.
Yes
The Rev. 1 CIP-007, 008, and 009 standard requirements are largely consistent with the Control Center/SCADA/EMS operating environment. The requirements of these standards are new to generating plant and substation environments. The project should better address the application of CIP-005, CIP-007, CIP-008, and CIP-009 to generation plants and substations, and if appropriate include development of guidance or reference to NIST SP800 series reports.
Group
WECC Critical Infrastructure and Information Management Subcommittee (CIIMS)
Robert Mathews
Pacific Gas and Electric Company
1 - Transmission Owners
(415) 973-0609
rpm4@pge.com

Dave Ambrose
Dave Ambrose
WAPA - Loveland
WAPA - Loveland
WECC, WECC
3, 1, 3, 1
Vern Kissner
Vern Kissner
Tacoma Power
Tacoma Power
WECC, WECC
Marc DeNarie
Marc DeNarie
WAPA - Folsom
WAPA - Folsom
WECC, WECC
3, 1, 3, 1
Jeff Mantong
Jeff Mantong
WAPA - Folsom
WAPA - Folsom
WECC, WECC
3, 1, 3, 1
Gray Wright
Gray Wright
Sierra Pacific Power
Sierra Pacific Power
WECC, WECC
3, 5, 1, 3, 5, 1
Jamey Sample
Jamey Sample
CAISO
CAISO
WECC, WECC
2, 2
No
Please see specific items in questions 2, 4, and 5.
No
Paragraph 4 of the SAR isn't clear. Assuming that the proposal of this paragraph, and it's bullets, is directly related to FERC Order 706 Paragraph 272, we would recommend rewording to: "This SAR will provide clairty in identifing various types of assets that feed information to critical assets used to support the reliability and operability of the Bulk-Power System as directed in FERC Order 706 Paragraph 272. This includes how to addess: - Regional Entities and Purchasing-Selling Entity functions as they relate to the reliability and operability of the Bulk-Power System. - Reliability and Market Interface Principle 4 (plans for emergency operations and system restoration).
None
None
No
In theory it is a reasonable approach if the first phase only consist of simple changes to reporting timeframes, etc. that don't have any interrelation or complexity to controveral topics. Then phase two be addressed as a whole versus multiple interations. This is because we feel that multiple interations will only increase the oveall administrative burden on the drafting team, increase complexity of an already complex task, possibably result in throw awary work, and impact our ability to deliver a cohesive, quality, and timely product.
Yes

In general the industry seems to still be challenged in situations where there are hybrid devices that use both serial and routable protocols. An example is where a Critical Cyber Asset is a serial device which is connected directly to a router, thus converting it to a routable protocol. The SAR should include explicity address these types of situations. We are not recommending that we expand the current CIP scope to include serial devices, but rather explicit guidance.
1)Suggest that FERC be an active participant in drafing both the CIP 2-9 SAR and subsequent standards revisions 2) Emphasize the need for the scope of the revisions to CIP002 to adress the need for a consistent framework to identify critical assets.
Individual
Gerald Freese
American Electric Power
(614) 716-2351
gsfreese@aep.com
ERCOT, RFC, SPP
3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators , 1 - Transmission Owners
Yes
Yes
Yes
Logical progression.
No
Individual
Paul Kerr
Coral Power, L.L.C.
(519) 620-7712
paul.kerr@shell.com
SPP, SERC, WECC, RFC, MRO, NPCC, ERCOT
6 - Electicity Brokers, Aggregators
Yes
Assuming the question should read: "Do you agree with the scope of the proposed standards action ?" The scope of the SAR is reasonable, since it is to address the directives of Order 706. Yet, this needs to be differentiated from the proposal in the SAR to expand the scope of applicable entities to include the Regional Entity and Purchasing-selling Entity. Inclusion of PSEs was not directed in the Order, or even considered as part of the NOPR, and should be removed from the SAR.
No
Making the standards applicable to the Regional Entity function was in the NOPR, commented on by stakeholders, considered by FERC and determined to be appropriate (paragraph 47). A great deal of discussion and consideration went to addressing comments and concerns regarding demand side aggregators, concluding with the direction that NERC should consider whether there is a need to register such entities and, if so, to address related issues and develop criteria for their registration (paragraph 51). As such, it is easy to agree that the applicability sections of the standards should be changed in line with the Order. However, nowhere, in this Order or in the NOPR, did FERC propose or contemplate or even discuss the inclusion of PSEs as responsible entities for the CIP standards. If there were any concerns related to PSEs they would have been raised by FERC and/or pursued by stakeholders, similar to those regarding small entities. FERC considered this, and determined that it would be "overly-expansive" to require every entity connected to the Bulk-Power System, to comply with the CIP standards, regardless of size (paragraph 49). PSEs, of course, are not even connected to the BPS. In reaffirming its reliance on the NERC registration process to identify entities that should comply with the CIP standards, FERC was not directing NERC to go back and make them apply to more entities, like PSEs. On the contrary, in listing all of the responsible entities that must comply with the CIP standards in paragraph 31, it is clear that FERC knew exactly which entities the standards do not - and should not - apply to. There is no explanation or support within the SAR describing the logic or reliability reasons for making PSEs responsible entities under the CIP standards. The only justification appears to be the desire to address the directives of FERC in Order 706, but there is no such directive to include PSEs. The SAR should be amended to eliminate the expansion of the applicability to PSEs.

Yes
no comment
none
Individual
Eric Olson
Transmission Agency of Northern California
(916) 852-1673
eolson@navigantconsulting.com
WECC
1 - Transmission Owners
The Transmission Agency of Northern California (“TANC”) appreciates the opportunity to comment on this SAR. TANC believes that the applicability of the Cyber Security Standards (i.e. CIP-002-1 through CIP-009-1) to Transmission Service Providers (“TSP”) is inappropriate and unnecessarily burdensome on entities registered as TSP, and thereby requests that this applicability be removed in the revised standards. FERC Order 706 conditionally approved the current versions of the Cyber Security Standards and directed modifications to the standards that are initiated by this SAR. In Order 706 at Paragraph 49, FERC cautions against an "overly-expansive" approach "requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry." TANC contends that business practices related to the TSP function do not involve any Critical Cyber Assets and therefore concludes that the current TSP applicability of the revised standards is inappropriate. In its "Glossary of Terms Used in Reliability Standards" as adopted by the NERC Board of Trustees on February 12, 2008, NERC provides the following definitions of terms essential to the applicability of the CIP standards: Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data. Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets. The TSP’s primary functions are administering the transmission tariff and processing transmission service requests in accordance with its tariff and transmission service agreements. In this capacity, the TSP calculates Available Transfer Capability, approves transmission service requests from customers, and validates e-tags received from the Interchange Authority for confirmation that the interchange schedule references a valid transmission reservation. Computer systems used by the TSP are limited to the OASIS and e-tagging systems, both of which are typically third-party hosted web-based applications. Many TSPs use a common third-party vendor for these systems. As these systems are typically hosted externally to the TSP, there are no Critical Cyber Assets necessarily owned by the TSP, and applying the CIP standards individually to TSPs imposes unnecessary costs of compliance on these entities. It is also unlikely that degradation of these systems used by the TSP would affect the reliability or operability of the Bulk Electric System because these systems are not involved in actual Bulk Electric System operations. The NERC Functional Model (Version 3) states that the Transmission Service Provider does not itself have a role in maintaining system reliability in real time – that is the Reliability Coordinator’s and Transmission Operator’s responsibility. The TSP’s systems support commercial activities involved in the administration of the transmission tariff and forward planning activities (information related to facility ratings and transfer capabilities) that do not pose the same degree of risk to reliability as systems involved in transmission system operations, monitoring and controls. Continuing to include TSP in the applicability section of the revised standards causes every entity registered as TSP to comply with the requirements of CIP-002 only to annually confirm that they have no Critical Cyber Assets related to that function. Such an exercise would be unnecessarily burdensome to entities that are already incurring high costs to comply with the appropriately applicable standards.
Individual
Michael Puscas
United Illuminating
(203) 926-5245
michael.puscas@uinet.com
NPCC
1 - Transmission Owners, 3 - Load-serving Entities
Yes

Yes
Yes
No
Group
National Institute of Standards and Technology
Keith Stouffer
National Institute of Standards and Technology
9 - Federal, State, Provincial Regulatory, or other Government Entities
(301) 975-3877
keith.stouffer@nist.gov
Stu Katzke
Stu Katzke
NIST
NIST
NA - Not Applicable, NA - Not Applicable
9, 9
Marshall Abrams
Marshall Abrams
Mitre
Mitre
NA - Not Applicable, NA - Not Applicable
NA, NA
No
NIST agrees with the proposed changes in FERC Order 706 and proposes several additional items for consideration listed in the comments section of Question 5 of this comment form.
Yes
Yes
Yes
General Comments Summary: NIST believes that if the changes specified in FERC Order 706 and the recommendations below are implemented, NERC will have made a positive step towards making the CIPs commensurate with the NIST SP 800-53, Rev 2 moderate baseline. However, there are still differences in coverage and in the level of specificity of the security requirements that need to be addressed. NIST would also like to point out that many of the federal agencies that own/operate industrial control systems in the bulk electric sector are classifying their systems as High impact systems that implement the High baseline requirements in SP 800-53. NIST is willing and has the resources to work on the NERC standards team in developing the next revision to the standard. Approach: Critical Assets vs Information System NIST understands that in the electric sector, protecting critical assets has been the predominant paradigm, but recommends for future revisions of the standards that an information systems approach rather than critical asset approach be considered. Our rational for this suggestion is as follows: While it is important to identify critical assets using a risk-based assessment methodology, NIST suggests that NERC consider applicability of the CIPs at an information system level rather than at the critical asset level. An information system view provides a more natural context for the application of information technology security across an industrial control system composed of multiple components, where some subset of the components is supported by information technology. Under the current scope of the CIPs, all of the CIP security requirements would be applied to every critical cyber asset. In some cases, application of all of

the CIP security requirements to a critical cyber asset may not make sense or may be excessive due to the nature of the asset. When an information system view is adopted, the CIP security requirements would be applied at the information system level, resulting in the allocation of CIP requirements to specific components. All components of the information system are not required to support every information system security requirement—just those that are identified as a result of the requirement allocations; thus resulting in significant cost savings. Using the information system view, there is no need to distinguish between cyber assets and critical cyber assets as all cyber assets within the information system are protected. Comments on Specific Requirements CIP 002 R3.1 NIST strongly recommends that a clear unambiguous definition of “routable protocol” be developed and, based on that definition, all routable protocols currently within the scope of the CIPs should be identified. All data encapsulated within a routable protocol should also be within the scope of the CIPs. CIP 002 R3.2 NIST recommends that “control center” should be replaced by “electronic security perimeter.” Nuclear Facility Exemption In reference to section 4.2.1 of each CIP, NIST observes that the electric side of nuclear power plants can have an impact on the bulk electric sector. NIST suggests that the continuity of power aspects of nuclear facilities should be included in the scope of these standards. Therefore NIST recommends that the exemption statement “Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission” be changed to “Specific systems that are regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission (e.g., safety systems)." Wireless NIST observes that the CIPs do not sufficiently address the security of wireless technologies, which include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth.. There appears to be an assumption in the CIPs that communication occurs solely over media. Consequently, NIST recommends that a clear, unambiguous definition of wireless technology be developed and security requirements for wireless technologies be included in the CIPs. Media Protection NIST recommends that the CIPs’ media protection requirements be expanded to cover all types of media. Because of the miniaturization and increased portability of digital media, protection of this media by a physical security perimeter is no longer adequate. Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). Information system media are also components of portable and mobile computing and communications devices (e.g., notebook computers, personal digital assistants, cellular telephones). The organization should have policy and procedures to protect and control information system media during transport outside the physical perimeter and restrict the activities associated with transport of such media to authorized personnel. For example, many organizations today prohibit removing laptop computers with unencrypted hard drives from the physical protection perimeter, and enforce this policy with unannounced inspection at the exits. Information system media is also a component of telephone systems that have the capability to store information (e.g., voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, policy should address the types of information stored on telephone voicemail systems that are accessible outside of physically protected areas.
Individual
Thad Ness
AEP
614-716-2053
tkness@aep.com
ERCOT, RFC, SPP
5 - Electric Generators, 6 - Electicity Brokers, Aggregators , 1 - Transmission Owners, 3 - Load-serving Entities
Yes
No
In general a PSE has no direct control on system (e.g. OASIS, organized Market Applications) and/or the grid, and relevant transactions are ultimately approved or denied by a current reliability function such as the Interchange Authority, Balancing Authority and Reliability Coordinator. The PSE function was originally (and still is) designed in the context of the physical scheduling process to assign financial responsibility in the related contract path represented on an eTAG. A PSE neither creates load or generation, and at all times only serves as an intermediary, in a bilateral transaction, to schedule generation to load. There is already enormous confusion as to what an LSE does (Market based functions vs. Reliability based functions), and in reality, what FERC references in Order 706 best aligns with the LSE function, definitely not a PSE function, so lets not further confuse the issue by wrongly including the PSE function in this debate.
Yes
It should be well established that the standards revisions are not to be construed as standards re-writing. The basic concepts except as noted by FERC in the final rule should stand.
No

Individual
William Lucas
We Energies
(414) 221-2220
william.lucas@we-energies.com
RFC
3 - Load-serving Entities, 5 - Electric Generators
Yes
We Energies feels that incorporating the FERC 706 directives will privide additional clarity around implementation requirements and compliance measures to the existing CIP 002-009 standards.
Yes
We Energies is not aware of any regional or business variance that the standards team should consider.
Yes
We Energies would like to see the drafting team address modifications as they apply to any requirement(s) throughout the standard set.
Yes
Compliance dates for any additional critical assets that need to be included as a result of the revised standards, or any new requirements for existing critical assets will require extended dates for compliance. The FERC 706 order will create changes in the NERC CIP requirements that will most likely be approved after some of the existing compliance dates have passed.
Group
NPCC Regional Standards Committee
Lee Pedowicz
NPCC
10 - Regional Reliability Organizations/Regional Entities
212-840-1070
Lpedowicz@npcc.org
Guy Zito
Guy Zito
NPCC
NPCC
NPCC, NPCC
10, 10
Brian Hogue
Brian Hogue
NPCC
NPCC
NPCC, NPCC
10, 10
David Kiguel
David Kiguel
Hydro One
Hydro One
NPCC, NPCC
3, 1, 3, 1
Kathleen Goodman
Kathleen Goodman
ISO New England
ISO New England

NPCC, NPCC
2, 2
Ben Li
Ben Li
Independent Electricity System Operator
Independent Electricity System Operator
NPCC, NPCC
2, 2
No
1. The SAR is not specific on which CIP standards are "low hanging fruit", which ones contain more contentious issues than the others. It does not identify a proposed implementation plan that would support multiple revisions to the standards, whereas some changes would be reviewed by industry, balloted, and submitted for approval. 2. The SAR indicates that if additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator--see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely directed "…that NERC should register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System." In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model as long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. In this case, we expect the "Demand Side Aggregator", which we believe performs the tasks listed under the LSE in the model, will register as an LSE. Hence, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this speculative revision to scope statement should be in the SAR. 3. The originating cause and this SAR's scope should not be limited to FERC Order 706. Experiences from stakeholder's implementing the Cyber Standards should be taken into consideration as lessons learned as part of the scope for developing Standards. Extending the SAR beyond FERC Order 706 should only be done if it will not affect timelines given by FERC. Also, interpretations made subsequent to the standards should be formally codified into the appropriate places in the standards, such as the CIP-006 interpretation and any FAQ interpretations.
No
The SAR should remove the applicability to the RE. The RE is not a user owner or operator and does not have Critical Cyber Assets that control the BPS. We do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order. With respect to the proposed to make conforming changes to the cyber security standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please refer to the comments above in Question 1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.

No
While we support this as a general approach when NERC develops several standards at the same time, we are unable to further comment on its merit absent any proposed implementaiton plan and any indication in the SAR as to which standards are "low fruit dropping" and which ones are more controversial than the others. We would suggest, however, that the inter-relationship among these standards be considered in developing the staged implementation plan. We recommend that the SAR be broken into two or more SARs. The first SAR can address the "low hanging," less contentious issues. A second SAR can address the more contentious issues.
Yes
We do not want to limit the SAR to 706. We suggest that: 1) the inclusion/exclusion of Generation should be clarified 2) either delete CIP-001 or add it to CIP-008 3) add the definition of a control center 4) clarify that if a control center has a backup that demonstrates the control center's criticality, then the control center should be considered a Critical Asset
Of concern is the one size fits all approach by the standards, in that many requirements attempt to address themselves equally to several different cyber environments. NPCC sees major differences with respect to control

center environments and configurations, which are more like typical IT Enterprise style environments utilizing readily available hardware, software, and application platforms and processes. Generators, substations, and other small or remote facilities, have older legacy and single function system and process configurations, which can be best described as atypical to control room configurations. The problem lies in the difficulty of trying to define technical requirements that can effectively address the different kinds of cyber environments. The result too often is a requirement that serves no one environment well. The standards attempt to resolve this by leaving it to the Entity to try and figure out what the real requirement is for them, and wondering whether their implementation will be compliant. Therefore NPCC believes that such requirements need to specify which cyber environments they apply to, and ensure they provide appropriate clarity and direction to that environment.
Group
Southern Company - Transmission
Jim Busbin
Southern Company Services, Inc.
1 - Transmission Owners
(205) 257-6357
jybusbin@southernco.com
J. T. Wood
J. T. Wood
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Roman Carter
Roman Carter
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Marc Butts
Marc Butts
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Jay Cribb
Jay Cribb
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Valerie Piazza
Valerie Piazza
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Yes
Please see our response to Question #2.
Yes
We agree with the RE and PSE additions if it makes sense. However, if the drafting team feels that this is not appropriate remove it As to the DSM function, it appears that this is just a subset of the LSE function and this is just a market function. The drafting team should consider if this is a duplicative function of the LSE.
We know of no regional variances to identify at this point. However, if at some point in time the drafting team feels one is necessary they should consider adding it.

Yes
It is our understanding that the SAR drafting team will consider the directives from the FERC order first and establish a priority level. The less contentious and less complicated items are assumed to be considered first for quick turnaround, followed by the more difficult issues.
Yes
For the future, implementation plan(s) should be reviewed to determine overlapping and interrelated issues of timing and revised appropriately (e.g. CIP-004, CIP-005 & CIP-006 may need to have requirements listed in better order so that background checks and training is done 'after' the electronic and physical perimeters are defined). Need flexibility to apply emerging technologies that improve the reliability of the bulk electric system rather than reducing reliability just to comply with the CIP standards. Need more granularities to the term "critical". There are indeed levels of criticality but these are not captured in the current standards. In much of the comments concerning NERC's CIP standards, one of the main objections raised is the great degree of flexibility in determining what assets are within scope. However from a utility viewpoint, the main issue with the NERC CIP standards is actually their inflexibility. With all the talk of choosing our own assets using 'risk based methodologies', 'reasonable business judgment', 'technical exceptions', and 'acceptance of risk' it may be surprising to hear that anyone feels the standards are inflexible. However, the CIP-003 to CIP-009 standards are clearly written to apply to control room data centers and the types of cyber assets contained within them. These standards, which are appropriate for that environment, are then broadly applied to assets in the field such as substations and plants. The standards are inflexible in that they require this data-center like security around assets that are located in environments that are nothing like a data center. This base tension between data center environments and field environments is the reason that such flexibility must be included in CIP-002 and then sprinkled throughout the others. The issue with CIP-002 is actually in the inflexibility of CIP-003 to CIP-009. If the standard and its existing requirements were to be scoped to data-center environments for control systems, the standard would need much less flexibility throughout. A separate set of standards could then be developed through the NERC process that is more appropriate for assets located in the field. But with a scope of 'anything with a chip in it located anywhere in your service territory' then much flexibility is required. The CIP-002 standard only allows two classes of assets – a cyber asset is either 'critical' and is to be protected to data-center level security or its 'not-critical' and is out of scope. The standard allows no middle ground, no 'risk based' protection, absolutely no flexibility in protecting those assets that fall somewhere in-between. It is purely binary. It is analogous to writing security standards appropriate for the cash processing operations of the central Federal Reserve banks that handle massive amounts of cash and then forcing them to apply to every location which houses any cash whatsoever, including all ATM's located in the field. The cost is prohibitive, you actually hinder the legitimate use of the asset, and the decrease in risk for the majority of the assets covered is negligible. For the most part, this tension revolves around the physical security and personnel aspects of the standard and their implementation for field locations. The standards go outside of typical technical, electronic access cyber security issues and enforce physical security and personnel-oriented security issues in a cyber asset focused vacuum. One cannot look at personnel or physical security issues holistically even on a site basis; no it must be focused solely on a particular cyber asset. This forces the industry to do costly things that bring little to no benefit or risk reduction and waste resources solely to be compliant to an inflexible standard that could be better spent reducing larger security vulnerabilities elsewhere. This is what causes most of the consternation and the desire to maintain great degrees of flexibility and control scopes within these standards.
We'd ask NERC to consider informing the industry early and often as to the various drafting options you would consider on these CIP standards.
Individual
George W. Brady
Ohio Valley Electric Corporation
(740)289-7297
gbrady@ovec.com
RFC
1 - Transmission Owners
No
No
Regional Entities are not users, owners or operators of the Bulk Electric System and thus the reliability standards do not apply to them by definition. It is not clear why the LSE and PSE are to be included. LSEs and PSEs do not own any Critical Assests that directly affect the bulk electric system. Subsequently, these entities could not have any Critical Cyber Assets.
No

Registered entities have already been working towards compliance with the CIP standards per the existing implementation plan. The drafting team is now proposing to make changes before the existing implementation plan is complete. Registered entities need to be allowed to become compliant with the existing standards before additional changes are made to the CIP standards. Otherwise, the drafting team is creating a moving target that provides an incentive to delay implementation right up until an entity is required to be auditably compliant. By delaying their implementation, registered entities could save costs from having to make multiple changes to meet changing CIP requirements without incurring penalites. FERC confirmed in Order 706 that no penalties could be applied until the auditably compliant phase. The drafting team should list the required changes from FERC Order 706 directly in the SAR and what class they consider the change to be in. Also, if additional and acceptable changes are requested from the commentors, these changes should be listed in the SAR and clearly marked as coming from industry.
Yes
How do the standards apply when a new Critical Cyber Asset is deployed? Is there a grace period to bring it into compliance? The drafting team should address this issue.
Group
Compliance Department
Patrick Miller
Western Electricity Coordinating Council
10 - Regional Reliability Organizations/Regional Entities
(360) 567-4056
pmiller@wecc.biz
Yes
Yes
Yes
This may be more difficult than it seems, but the approach is a good idea and should be allowed. There may be issues that seem easier than others at the onset of the effort which could ultimately end up being far more contentious than originally expected. Greater success may be found if there is a defined process for flexibility around these unforeseen challenges such as a transition mechanism from the "easy" to "hard" range.
Yes
WECC would like to see additional clarity around CIP-003-01.R3, specifically with respect to the difference between exception to policy and exception based on technical feasibility. Additionally, any potential situations other than technical feasibility which may commonly warrant exception should also be clarified within this effort. WECC agrees with FERC and the Blackout Report (FERC CIP NOPR, paragraph 139) that inappropriate disclosure of information should be prevented. This matter could be clarified by improving the language in CIP-003-01.R4 to describe the type of "protection" required. For example, language around digital protection such as encryption (at rest and in transit) for data elements and physical protections such as locked storage for maps, diagrams and other printed materials could be added. Additionally, verbiage describing if/how the information relevant to CIP-003-01.R4 is/isn't "data" that should be classified as a Critical Cyber Asset per the definition(s) provided in the NERC Glossary would be beneficial. Based on feedback from Registered Entities, there appears to be some confusion around how the requirements within CIP-005-01.R1.3 and CIP-006-01.R1.1 relate to one another. The crux of the issue is whether or not an entity can create one large Electronic Security Perimeter using Virtual Private Network (VPN) or similar technology to act as a "conduit" between physical facilities, or if they should maintain an individual Electronic Security Perimeter at each physical facility within a Physical Security Perimeter. WECC requests additions to the relevant CIP standards providing sufficient direction in this area.
WECC recognizes and supports the shift toward standards that more closely align with the NIST SP800 series. Opportunities during this revision effort should be taken to move the existing CIP standards in that direction. Inclusion of appropriate elements from various Special Publications, and not just SP800-53x, should be considered since there is overlap and interplay between the various SP800 documents. WECC acknowledges the importance of protecting Critical Cyber Assets, however, at some point in time if not part of this revision process, physical security of the Critical Assets must be addressed.
Individual
Greg Rowland

Duke Energy
(704)382-5348
gdrowland@dukeenergy.com
RFC, SERC
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
No
While we agree for the most part with the scope, the Critical Assets are generally Control Centers, Substations, and Critical Generation. What applicability does this standard have for LSE? Is it appropriate that LSE's are included?
Yes
No
We are concerned about how "easy" versus "contensious" issues will be identified. Furthermore a staggered approach will add complexity to corresponding changes that must be made to the implementation plan. The SDT should consider getting all changes in one revision to simplify the process.
No
However the House Subcommittee concerns about critical infrastructure protection are not addressed. After implementing FERC's direction the CIP standards will still only cover a small fraction of the assets identified by the House Subcommittee. Because of this, the CIP standards will continue to come under criticism.
It appeared that the original drafting team had a strong focus on Energy Management systems supporting Control Centers. When the same CIP standards were applied to Substations, some of the requirements, i.e., patch management, anti virus, etc., had limited applicability. Additional specific expertise is needed on the drafting team to ensure the standards are equally applicable to all relevant Critical Assets. Any changes (particularly in the identification of Critical Assets) MUST include corresponding changes to the implementation plan.
Group
Midwest ISO Standards Collaborators
Jason L. Marshall
Midwest ISO
2 - RTOs and ISOs
317-249-5494
jmarshall@midwestiso.org
Joe Knight
Joe Knight
Great River Energy
Great River Energy
MRO, MRO
1, 1
Kirit Shah
Kirit Shah
Ameren
Ameren
SERC, SERC
1, 1
Joeseph DePoorter
Joeseph DePoorter
Madison Gas and Electric Company
Madison Gas and Electric Company
MRO, MRO
6, 3, 4, 5, 6, 3, 4, 5
No
See our answers to the other questions.
No

Regional Entities are not users, owners or operators of the Bulk Electric System. Thus, reliability standards can't apply to them by statute. It is not clear why the LSE and PSE are included. The LSE and PSE will not own any Cyber Assets that directly affect Critical Assets. Thus, it is not possible for them to have Critical Cyber Assets.
No
Registered entities have already been working towards compliance with the CIP standards per the existing implementation plan. Now, this drafting team is proposing to make changes before the existing implementation plan is complete. Registered entities need to be allowed to become compliant to the existing standards. Afterward, then additional changes can be made to the CIP standards. Otherwise, the drafting team is creating a moving target that provides an incentive to delay implementation right up until an entity is required to be auditably compliant. By delaying their implementation, registered entities could save costs from having to make multiple changes to meet changing CIP requirements without incurring penalites. FERC confirmed in order 706 that no penalties could be applied until the auditably compliant phase. We also believe that the drafting team should list the required changes from FERC Order 706 directly in the SAR and what class they consider the change to be in (i.e. low hanging fruit,etc.) Also, if additional acceptable changes are requested from the commenters, these changes should be listed in the SAR and clearly marked as coming from industry.
Yes
How do the standards apply when a new Critical Cyber Asset is deployed? Is there a grace period to bring it into compliance? The drafting team should address this issue.
Group
Dominion - Electric Market Policy
Louis Slade
Dominion Resources Services, Inc.
3 - Load-serving Entities, 6 - Electicity Brokers, Aggregators , 5 - Electric Generators
(804) 273-2461
louis.slade@dom.com
Harold Adams
Harold Adams
RFC, RFC
3, 5, 6, 3, 5, 6
Jalal Babik
Jalal Babik
SERC, SERC
3, 5, 6, 3, 5, 6
Yes
No
The FERC order stated "that demand side aggregators might also need to be included in the NERC registration process if their load shedding capacity would affect the reliability or operability of the Bulk-Power System. The current version of NERC functional model definition of PSE does not contain any reference to load shed capability, which is the focus of FERC's comment. As we've stated in comments to other standards, the ability to shed load lies with the asset owner of the physical infrastructure.
Yes
No

Individual
Denise Roeder
ElectriCities of North Carolina, Inc.
(919) 760-6255
droeder@electricities.org
SERC
6 - Electicity Brokers, Aggregators , 4 - Transmission-dependent Utilities, 3 - Load-serving Entities
Yes
However, do not agree with expanding the scope of applicability as stated (see response to Q2).
No
By definition, the PSE purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. To accomplish that, it would have to work through other entities (TSPs, BAs, TOPs, GOPs, etc.) that are already required to meet the cyber security standards and that DO have responsibilities for managing and operating the facilities and processes that actually impact the reliability of the BES. If the PSE happens to be an affiliated merchant or a generator owner itself, then in addition to being registered as a PSE, that entity should also be registered according to the other functions it performs and would have to comply with the cyber security standards on those registration bases. It does not make sense to extend registration to PSEs, or any other functional entity, whose function itself does not physically impact the reliability of the BES.
Yes
As long as it is perfectly clear to all stakeholders at any time which modifications are under review, which are being balloted, and which are being submitted for approval.
No
Group
Public Service Commission of South Carolina
Phil Riley
Public Service Commission of South Carolina
9 - Federal, State, Provincial Regulatory, or other Government Entities
(803) 896-5154
philip.riley@psc.sc.gov
Yes
Yes
Yes
No
Individual
Greg Ward / Steve Martin
Oncor Electric Delivery Company LLC
(214) 743-6862
steve.martin@oncor.com
ERCOT
1 - Transmission Owners
No

No
Oncor Electric Delivery does not agree that the Demand Side Aggregator should be a registered Entity subject to the NERC CIP standard. For purposes of Load Shedding within ERCOT, Oncor Electric Delivery performs this function as directed in ERCOT's Guides and Protocols.
Yes
No
Individual
Ron Falsetti
Ontario IESO
(905) 855-6496
ron.falsetti@ieso.ca
NPCC
2 - RTOs and ISOs
No
1. The SAR is not specific on which CIP standards are "low hanging fruit", which ones contain more contentious issues than the others, and any proposed implementation plan that supports multiple revisions to the standards while some changes are reviewed by industry, balloted, and submitted for approval. 2. The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator – see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely dircted [….NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.] In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model for so long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. In this case, we expect the "Demand Side Aggregator", which we believe performs the tasks listed under the LSE in the model, will register as an LSE. Hence, we do not expect the functional model to be revised in order to address this directive. As a result, we do not agree that this speculative revision to the scope statement should be included in the SAR.
No
We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling Entities. Regional Reliability Organizations were included as applicable entities in the previously submitted CIP standards; the proposal to include the RE is a only matter of name change with respect to the revised Functional Model. However, we do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order. With respect to the proposal to make conforming changes to the cyber security standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see our comments on Q1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.
No
We do not agree with the "multi-phase" approach. Such an approach brings out multiple concerns - which set of standards should we begin to focus our attention on while developing implementation plans as these cannot be developed and implemented overnight - what if we or any other applicable entity begin work on a set of standards which ultimately gets voted down by the industry - should we wait to see which set of standards gets the assent which would mean delays in the implementation phases - what factors decide which set of standards go through - would this not bring into the forefront issues related to costs and risk mitigation. There are too many questions that would remain if such an approach were to be applied. We strongly suggest that all these standards be developed and implemented at the same time to avoid confusion. If it becomes necessary to implement these standards in

stages, we urge the SDT to consider the inter-relationship among these standards and clearly convey the rationale for a staged implementation plan.
No
The four tables in the Implementation Plan prescribe the initial compliance schedule for a registered entity, with Table 4 addressing new entities that register in the future. But there is no table prescribing a schedule in which an existing registered entity can bring a newly identified critical asset and its critical cyber assets into compliance. While not expected to change frequently, the critical asset list can change for any number of valid reasons, and the registered entity needs to have an appropriate period of time in which to achieve compliance with the standards for that asset. In the absence of a compliance schedule, no guidance is available to either the registered entity or the auditor. A new table should be developed defining a compliance schedule for standards CIP-003 through CIP-009 applicable to newly identified critical assets and based upon the date of the risk assessment. The new table should give due consideration to those CIP requirements that are broadly applicable to the entity and should already be in compliance, and those requirements that require new resources and effort and should be afforded adequate time to reach compliance. That consideration should include consideration whether or not the entity had previously identified any critical assets. The applicability of the standards should be expanded to include LSEs which own BES transmission and/or distribution facilities.
Individual
Ken Welch
LK4 Technology Corporation
866-586-8732
kw1@lk4technology.com
NA - Not Applicable
Not Applicable
Yes
The industry needs to adopt a common risk assessment methodology. As a veteran compliance auditor for FFIEC, GLBA and SarBox, I have seen entire compliance programs disallowed because they did not start with the risk assessment. The NRC recently commissioned a cybersecurity risk assessment program and is in the process of commissioning a physical risk assessment. These risk assessments can be personalized for each individual complying entity, but a core criteria must be met by all.
Yes
A cybersecurity system is only as strong as its weakest link. Having unaudited systems interfacing with complying systems represents a large identifiable risk.
Yes
However, adoption/adaptation of the FFIEC could be a model to speed the phases. The underlying ISO requirements are identical.
Yes
Proof of policy relating to risk assessment produces "Auditable Compliance". This was the standard adopted decades ago by the National Security Agency and then NIST.
Group
PacifiCorp
WECC-NERC PMO@pacificorp.com
PacifiCorp
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators
503.813.5219
WECC-NERCPMO@PacifiCorp.com
WECC, WECC
Yes
Specifically, the scope needs to assure that the NIST standards are considered. Such standards will hlep organizations overcome confusion where elements of the existing standard is unclear.

NIST 800-82, NIST 800-53 and the catalog of control systems Security: Recommended for Standards Developers (Dept of Homeland Security)
Yes
The order as written does not adequately address the common security practice of using ste-to-site VPN technologies to extend a trusted security zone across multiple locations. With respect to the CIPRS,where the VPN endpoints are under the sole control of and within the Physical Security Perimeters of the same responsible entity, a properly configured VPN should be considered adequate mitigation of physical attacks against the communications link.
Individual
David Kiguel
Hydro One Networks Inc.
416-345-5313
David.Kiguel@HydroOne.com
NPCC
3 - Load-serving Entities, 1 - Transmission Owners
No
(a) The SAR is not specific on which CIP standards contain more contentious issues than the others, and any proposed implementation plan that supports multiple revisions to the standards while some changes are reviewed by industry, balloted, and submitted for approval. (b) The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (e.g. Demand Side Aggregator – see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. However, the FERC order has not asked NERC to revise its functional model; it merely directed NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk Power System. In our view, the "Demand Side Agregator" performs tasks that the FM lists under the LSE entity thus it should be registered as such. According to the above, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this revision to scope statement should be in the SAR.
No
(a) We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling Entities. However, clarification must be sought from FERC because Regional Entities are not Owners, Users or Operators of the BPS, thus not legally subject to reliability standards (b) We do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities and we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order. (c) With respect to the proposal to make conforming changes to the CIP standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see our comments in Question 1. Furthermore, we do not agree with the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We do not believe that changes the Compliance Registration Criteria would trigger a need to change the standards.
No
While this might be an acceptable approach, we are unable to further comment on its merit absent any proposed implementaiton plan and any indication in the SAR as to which standards are "low hanging fruit" and which ones are more controversial than the others. We would suggest, however, that inter-relationship among these standards be considered in developing the staged implementation plan. Alternatively, the SAR could be broken into several SARs one for each phase.
Yes
There is now an opportunity to extend the SAR's scope beyond the content in the FERC Order, provided that FERC timelines can still be met. Interpretations which were made subsequent to the standards should be formally codified into the appropriate places in the standards, such as the CIP-006 interpretation. Similarly, experience from entities implementing the Cyber Standards should be taken into consideration as there have been valuable lessons learned.

Group
FirstEnergy
Sam Ciccone
FirstEnergy Corp.
5 - Electric Generators, 6 - Electicity Brokers, Aggregators , 3 - Load-serving Entities, 1 - Transmission Owners
(330) 252-6383
sciccone@firstenergycorp.com
Terry Malone
Terry Malone
FE
FE
RFC, RFC
Doug Hohlbaugh
Doug Hohlbaugh
FE
FE
RFC, RFC
Dave Folk
Dave Folk
FE
FE
RFC, RFC
Rob Martinko
Rob Martinko
FE
FE
RFC, RFC
Henry Stevens
Henry Stevens
FE
FE
RFC, RFC
No
See our comments to the rest of the comment form, plus the following: 1. Although we agree the scope must address the FERC directed changes from Order 706, the SAR must be developed further and lay out a table of all the directives. We look at this first posting of the SAR as just a general starting point for the SAR drafting team who will further develop expectations for the standards drafting team. To aid the SAR drafting team and eventual standards development team, FE has tabulated the FERC directed changes in an Excel spreadsheet that we have submitted separately with these comments to NERC's Barbara Bogenrief. In addition, FE will provide more detailed guidance when the revised SAR is made available for comment. 2. It is not clear to FE how the FERC directed changes to the compliance elements such as Violation Factors and Violation Severity Levels will be handled by NERC staff or the eventual CIP standards drafting team. If they are to be addressed by the CIP standards drafting team, then changes to VRFs and VSLs should be included in the SAR scope.
Yes
The CIP standards should be adjusted to cover any and all functional entities that can impact the reliable operations of the BES. The CIP standards should be adjusted to focus on entities who own cyber entry points that can lead to a compromised BES. Presently the CIP-002 standard is focused on identification of critical BES assets (transmission/generation) and then reviewing those assets for critical cyber assets. This approach could exclude functional entities that do not own BES assets but have an impact on the reliable operation of BES assets.
Yes
Regarding the "multi-phase" approach and going after the "low hanging fruit" first, while that may be prudent, it is also important to quickly focus on modifications to CIP-002 since it drives all other CIP requirements. Also, by

changing CIP-002 first, the "critical asset list" will be focused solely on whether there is a true belief of BES criticality rather than be influenced by what an organization may have to do to secure the assets. The team should consider three phases: Phase 1: Handle the "urgent" issues for specific changes and timelines as directed by FERC (such as the removal of "reasonable business judgment" phrase from the standards). These could even be handled through separate "Urgent Action" SAR/Standard revisions as allowed by the NERC standard development process. Phase 2: Properly develop CIP-002 since this standard lays the groundwork for the other 7 CIP standards. Phase 3: Develop the rest of the requirements to CIP-003 through CIP-009 per the FERC directed modifications.
Yes
Although the Order discusses contractors and vendors, the standards may need more clarity with regard to how far a responsible entity must go to assure matters such as background checks are properly completed. The team should consider adding to the Scope of the SAR: "With regard to third-party vendors and contractors, provide clarification and additional guidance as to how much a responsible entity may rely on the processes and procedures of contractors and vendors that support the critical infrastructure of that responsible entity under the CIP standards and still be compliant with the standard."
FE provides the following additional comments: 1. The Scope will understandably address the FERC directed changes from Order 706. However, there may be instances in the Order where FERC believes a comment is valid but did not specifically direct a change but may merit a further look by the CIP drafting team. Also, as the drafting team work is underway, issues may arise and become more evident in the realm of critical infrastructure protection that may show a glaring need for new requirements. We want to assure that the SAR is not overly narrow in scope as to prevent the drafting team from proposing additional requirements that are both needed and sound. 2. Implementation - Throughout this development, the team should keep in mind that there is much work underway and completed by responsible entities in preparation for compliance with these standards as written today. Once changes are made, these entities should be given a reasonable amount of time to make any necessary adjustments. Furthermore, any new implementation schedule should start after the current implementation schedule is complete. 3. The SAR proposes to address the following NERC "principles": Reliability Principle 4 [Plans for emergency operation and system restoration of interconnected bulk electric systems shall be developed, coordinated, maintained and implemented] and Market Interface Principle 4 [An Organization Standard shall not preclude market solutions to achieving compliance with that standard]. It is not clear why the SAR should specifically address these principles. Are these not general principles applicable to every standard? If not, then why not address the other 6 Reliability principles and other 4 Market Interface principles? 4. NERC approved interpretation of CIP-006-1 R1.1, as well as ongoing interpretation development of CIP-006-1 R1.2 and CIP-005-1 Requirement 1 (per NERC project 2007-30) should be incorporated into the scope of the development of these standards. Also, in the SAR under "Industry Need", reference should be made to "CIP-006-1a" which has incorporated the NERC approved interpretation of R1.1 in Appendix 1.
Group
Electric Power Supply Association
Jack Cashin
Electric Power Supply Association
5 - Electric Generators
202-349-0155
jcashin@epsa.org
Yes
Yes. To the extent that the proposed SAR incorporates actions identified in FERC Order 706, the scope is appropriate. Given the recent, very thorough vetting of this issue through the FERC NOPR and Order process, the Standards Drafting Team should be very cautious about any extensions to that scope.
No
No. The SAR notes that based on a previous SAR, finalized on March 8, 2004, they intend to expand the applicability to include PSEs. EPSA does not agree with this addition. FERC Order 706 makes no suggestion that such an expansion of the applicability is appropriate. Indeed in Paragraph 31 of the Order, they note the 11 Functional Model entities that they believe are covered by the Order and PSEs are not included. If there was an intent to expand the applicability of the Standards, based on a 2004 SAR, it would have been appropriate to raise that issue during the FERC procedure.
The implementation plan provided to industry is resulting in some confusion and is open to different regional interpretations. Based on the title for Table 3, it should be applicable to Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators and Load-Serving Entities. Based on the title for Table 4, it is applicable to entities that registered in 2007. That leaves open to interpretation, the question of which Table applies to Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators and Load-

Serving Entities registered in 2007. Since Table 4 implementation dates are tied to the registration dates that were normally in the first half of 2007, entities forced to follow Table 4 would normally have 6-12 months less to achieve compliance. It appears that Table 4 was designed intentionally to give new registrants additional time to comply, but that due to the time used for regulatory processes, the result is the opposite. Namely, registrants have less time than otherwise similarly situated entities to comply with the standards. No justification exists for punishing the new registrants. Registered entities within the WECC region have been told that they are required to follow Table 4 if they were registered in 2007, while registered entities in the RFC region were told that if an entity had filed in “early 2007” they could follow Table 3. WECC registered entities were told that if they did not meet the milestone in Table 4 they are encouraged to file mitigation plans. This is an inconsistency across the regions that should be addressed. We recommend that the Standard Drafting Team be asked to remove this differentiation by eliminating Table 4 and, if necessary, expanding the applicability of Table 3 to include those entities registered in 2007.
Yes
No
no additional comments
Individual
Martin R. Hopper
M-S-R Public Power Agency
(408) 615-6677
msradmin@svpower.com
WECC
9 - Federal, State, Provincial Regulatory, or other Government Entities
No
See Question 2 comments.
No
M-S-R Public Power Agency ("M-S-R") has determined that the SAR's proposal to add Purchasing-Selling Entities ("PSE") to the applicability section of the revised standards is out of scope and inappropriate. NERC's announcement for this comment period states that "The SAR proposes to bring the following standards (i.e. CIP-002-1 through CIP-009-1) into conformance with the ERO Rules of Procedure and to address the directives from FERC Order 706," but our review of these documents finds no suggestions, let alone directives, indicating that these standards should become applicable to PSE. In Order 706 at Paragraph 49, FERC cautions against an "overly-expansive" approach "requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry." M-S-R contends that the PSE function in and of itself does not involve any Critical Assets, let alone Critical Cyber Assets and therefore concludes that the proposed PSE applicability of the revised standards is inappropriate. In its "Glossary of Terms Used in Reliability Standards" as adopted by the NERC Board of Trustees on February 12, 2008, NERC provides the following definitions of terms essential to the applicability of the CIP standards: Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data. Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets. While an entity's business practices related to the PSE function may involve confidential information related to power contracts and prices and this information may be resident on Cyber Assets, there is no manner in which these assets could affect the reliability or operability of the Bulk Electric System if destroyed, degraded, or otherwise rendered unavailable. Adding PSE to the applicability section of the revised standards would cause every entity registered as a PSE to comply with the requirements of CIP-002 only to annually confirm that it has no Critical Cyber Assets. Such an exercise would be unnecessarily burdensome to entities that are already incurring high costs to comply with the appropriately applicable standards.
None.
None.
No
M-S-R cannot agree with the "multi-phase" approach without knowing how the "easiest modifications" have been or will be identified. If adding PSE to the applicability section of the revised standards has been or could be considered an easy modification, then M-S-R is opposed to the "multi-phase" approach.
No
None.
Group
WECC - Critical Infrastructure and Information Management Subcommittee (CIIMS)

Robert Mathews - CIIMS Subcommittee Chair
WECC (Steve Rueckert)
10 - Regional Reliability Organizations/Regional Entities
415-973-0609
rpm4@pge.com
No
See specific items in questions 2, 4 & 5
No
Paragraph 4 of the Detailed Description section in the SAR isn't clear. Assuming that the intent of this paragraph is directly related to FERC Order 706 Paragraph 272, recommend revising the section to reflect that the scope of the drafting effort: “Provide clarity in identifying various types of assets that feed information to critical assets used to support the reliability and operability of the Bulk-Power System as directed in FERC Order 706 Paragraph 272. This includes how to address: - Regional Entities and Purchasing-Selling Entity functions as they relate to the reliability and operability of the Bulk-Power System. - Reliability and Market Interface Principle 4 (plans for emergency operations and system restoration).”
none
none
No
In theory, it is a reasonable approach if the first phase only consist of simple changes to reporting timeframes, etc. that don't have significant interrelation, complexity or controversial topics. Then phase two be addressed as a whole versus multiple iterations. This is because we feel that multiple iterations will only increase the overall administrative burden, increase complexity of an already complex task, possibly result in throw away work, and impact the ability to deliver a cohesive, quality, and timely product
Yes
SAR should include an item that CIP2-9 explictly addresses serial devices as the industry seems to be challenged in situations where there are hybrid devices that use both serial and routable protocols. An example is where a Critical Cyber Asset is a serial device connected directly to a router, thus converting it to a routable protocol. This is not a recommendation that the CIP2-9 scope be expanded to include serial devices, but that CIP2-9 provide explicit guidance.
1) Suggest that FERC be an active participant in drafting both the CIP 2-9 SAR and subsequent standards revisions if permissible 2) Emphasize the need for the scope of the revisions to CIP002 to address the need for a consistent framework to identify critical assets.
Group
ISO RTO Council Standards Review Committee
Charles Yeung
Southwest Power Pool
2 - RTOs and ISOs
832-724-6142
cyeung@spp.org
Patrick Brown
Patrick Brown
PM
PM
RFC, RFC
2, 2
Jim Castle
Jim Castle
NYISO
NYISO
NPCC, NPCC
2, 2
Ron Falsetti
Ron Falsetti
IESO

IESO
NPCC, NPCC
2, 2
Matt Goldberg
Matt Goldberg
ISO NE
ISO NE
NPCC, NPCC
2, 2
Brent Kingsford
Brent Kingsford
CAISO
CAISO
WECC, WECC
2, 2
Anita Lee
Anita Lee
AESO
AESO
WECC, WECC
2, 2
Steve Myers
Steve Myers
ERCOT
ERCOT
ERCOT, ERCOT
2, 2
Bill Phillips
Bill Phillips
MISO
MISO
RFC, RFC
2, 2
No
Comments: We generally agree with the scope of the SAR. However, we have the following clarifying questions/comments: The SAR should contain a complete, revised implementation plan for both current and proposed CIP implementation. The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator – see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely directed [….NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.] In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model for so long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. Hence, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this speculative revision to scope statement should be in the SAR.
No
Comments: We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling Entities. Regional Reliability Organizations were included as applicable entities in previously submitted CIP standards; the proposal to include the RE is a matter of name change. However, we do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on Critical Assets, nor can we find its inclusion stipulated in the FERC Order. Wrt the proposed to make conforming changes to the cyber security standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see

our comments on Q1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.
No
Comments: We do not agree with the multi-phased approach to implementation. The industry is already implementing the current CIP standards in a phased approach, implementing another series of revised standards in the same manner would only cause confusion as to which standards are applicable when and what is required. This approach also creates an incentive to wait as long a possible to become compliant. If a registered entity commits assets today to become compliant, it may have to commit more later to make modifications to meet the changes to the standards. However, if the registered entity waits until later phases of the implementation plan, it may commit less assets overall since it may avoid multiple investments. As long it complies by the auditably compliant phase, then they cannot be fined for non-compliance, per FERC Order 706.
Yes
Comments: The four tables in the Implementation Plan prescribe the initial compliance schedule for a registered entity, with Table 4 addressing new entities that register in the future. But there is no table prescribing a schedule in which an existing registered entity can bring a newly identified critical asset and its critical cyber assets into compliance. While not expected to change frequently, the critical asset list can change for any number of valid reasons (including new guidance from FERC, NERC or the Regional Entities as to what constitutes a "critical asset" for purposes of the CIP Standards), and the registered entity needs to have an appropriate period of time in which to achieve compliance with the standards for that asset. In the absence of a compliance schedule, no guidance is available to either the registered entity or the auditor. A new table should be developed defining a compliance schedule for standards CIP-003 through CIP-009 applicable to newly identified critical assets and based upon the date of the risk assessment. The new table should give due consideration to those CIP requirements that are broadly applicable to the entity and should already be in compliance, and those requirements that require new resources and effort and should be afforded adequate time to reach compliance. That consideration should include consideration whether or not the entity had previously identified any critical assets.
There is concern that entities have internal security measures in place that may exceed the CIP requirements. The SAR should include in its scope that the standard clarify measures for compliance will be relegated to the FERC approved requirements and not any internal policies.
Individual
Daniel Hecht
Sempra Energy Trading LLC and Sempra Energy Solutions LLC
(203) 355-5417
dhecht@sempratrading.com
ERCOT, FRCC, RFC, SPP, WECC, NPCC, MRO, SERC
6 - Electicity Brokers, Aggregators
No
Sempra Energy Trading LLC and Sempra Energy Solutions LLC disagree with the proposed changes to the applicability section of the Cyber Security Standards (CIP Standards). The expansion of the CIP Standards' applicability to Purchasing-Selling Entities (PSEs) would result in the unnecessary imposition of the CIP Standards on pure power marketers, which are typically registered only as PSEs. The overarching purpose of the CIP Standards is the identification and protection of Critical Cyber Assets, which are those "Cyber Assets essential to the reliable operation of Critical Assets." (The Glossary of Terms Used in Reliability Standards, May 2, 2007 at 4 (Glossary)defines Cyber Assets as "programmable electronic devices and communication networks including hardware, software, and data.") Entities that do not own or operate any Critical Assets have no Critical Cyber Assets and, therefore, should not be required to comply with the CIP Standards. Pure power marketers engage in power purchase and sale transactions, but do not own or operate any physical electric generation, transmission, or distribution facilities. They also do not own or operate any Critical Assets, which by definition are physical facilities connected to or integrated with the grid. (The Glossary defines Critical Assets as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.") As a result, pure power marketers do not own or operate any Critical Cyber Assets and, therefore, should not be required to comply with the CIP Standards. Although power marketers may be users of third-party electronic systems (e.g., OASIS or scheduling systems) that may be considered Critical Cyber Assets, such access is limited to user functions and does not allow in any way marketers (or any other users) to control those Critical Cyber Assets or the underlying physical Critical Assets. Pure power marketers

typically qualify and register only as PSEs. The proposed inclusion of PSEs in the applicability section of the CIP Standards would render the CIP Standards applicable to PSEs that are not also owners or operators of physical electric assets, such as power marketers. Such change would impose on such power marketers significant regulatory burdens and costs, without furthering the goals of the CIP Standards. Application of the CIP Standards should be limited to only those functional categories of entities that actually own or control physical electric assets that could be Critical Assets. Such entities are registered with NERC for the proper reliability function that results from the ownership or operation of physical electric assets (including Critical Assets), such as Generator Owner (GO), Generator Operator (GOP), Transmission Owner (TO), or Transmission Operator (TOP). To the extent GOs, GOPs, TOs, and TOPs are included in the applicability section of the CIP Standards, the current exclusion of PSEs from the CIP Standards does not result in any reliability gap, because owners or operators of Critical Cyber Assets are subject to the CIP Standards pursuant to the registration for the functions that relate to their ownership and operation of those physical assets. Indeed, if a power marketer contractually assumes responsibility for the reliability functions associated with the operation of a generator, that marketer will be required to add a GOP registration to its PSE registration. Thus, it appears that the only effect of revising the applicability section of the CIP Standards to include PSEs would be to impose on pure power marketers reliability standards that are not intended to apply to entities that do not own or operate any Critical Assets. The Commission has acknowledged that compliance with the CIP Standards may be difficult and burdensome and has provided for a three year phased implementation. Such burden should not be imposed on entities that do not own or operate Critical Assets and whose compliance with the CIP Standards would not further the reliability of the Bulk Electric System. In the alternative, if NERC revises the applicability section of the CIP Standards to include PSEs, it should qualify the term added in the applicability section to refer only to those PSEs that actually own or control physical electric assets. NERC has previously determined that it is in some cases appropriate to qualify the applicability of a standard to a functional category. For example, reliability standard PRC-016 applies to Transmission Owners, Generator Owners, and Distribution Providers, but its applicability is further limited to include only an entity “that owns [a Special Protections System].” As a result, the standard does not apply broadly (and unnecessarily) to every Transmission Owner, Generator Owner, and Distribution Provider. NERC should similarly consider adequate qualifications in the applicability section of the CIP Standards that clearly limit the applicability of the CIP standards to only those PSEs that own or operate physical electric assets.
No
See answer to Question 1

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

The Standards Committee thanks all commenters who submitted comments on the 1st draft of the SAR to revise the Cyber Security standards. These standards were posted for a 30-day public comment period from March 20, 2008 through April 19, 2009. The stakeholders were asked to provide feedback on the SAR through a special Standard Comment Form. There were more than 34 sets of comments, including comments from more than 100 different people from approximately 50 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

The 1st draft of the SAR focused on addressing the directives and recommendations contained in the FERC Order 706, and when posted, the drafting team asked stakeholders to identify any other issues encountered while attempting to follow the CIP standards. In response to stakeholder comments, the SAR DT made the following changes to the original SAR:

The SAR DT had proposed expanding the applicability of the existing standards to include requirements for the Regional Entity and the Purchasing-selling Entity. While most commenters agreed with the addition of the Regional Entity, most disagree with the addition of the Purchasing-selling Entity and the SAR was modified to remove the Purchasing-selling Entity as a responsible entity.

Most of the commenters agreed that the scope of the standards action to address the items identified in the FERC Order 706 is appropriate. Some went on to suggest that a list of these items accompany the SAR to which the SAR DT agreed.

There were many comments objecting to the reference to the Functional Model and the possible inclusion of requirements assigned to the "Demand Side Aggregator." Commenters indicated that the Load-serving Entity is already required to comply with the CIP standards, and the Load-serving Entity performs many of the same tasks as those assigned to the Demand Side Aggregator. Based on these comments, the drafting team removed the reference to the Functional Model and the Demand Side Aggregator from the revised SAR.

Some commenters suggested that the SAR be modified to include a specific reference to the Interpretation of CIP-006-1, and the drafting team has done so. As part of the standards process, the interpretation must be incorporated into a standard when it is revised.

Several commenters suggested that the Cyber Security Standard Drafting Team coordinate its work with other Cyber-related standards, guidelines and activities, and the SAR drafting team added the following to the SAR:

- Consider other cyber security related documents such as NIST, ISO 27000 Family, CIPC WG Risk Assessment Guideline, MITRE corporation technical report, DHS, National Laboratories papers, DOE 417, IEC, ISA, etc.
- Stay apprised of coordination work between FERC, NEI and NRC in regard to the Nuclear facility exemption issue with respect to regulatory gaps. As necessary modify the standards to reflect current determinations.

The following issues identified by stakeholders have been added to a list of issues for the standard drafting team to address and appended the list to the SAR as Attachment 3.

Industry Education

- Consider what to do with the existing FAQ document e.g., modify, replace.

- Consider how to provide additional guidance in support of these standards, e.g., Technical Reference documents, guidelines, white papers.
- Consider development of a guideline document to address extended LANs over multiple geographically dispersed locations.

Balloting and Implementation

- Determine the timing and grouping of revisions to be submitted to industry for comment and ballot, e.g., multi-phase or other approach.
- Determine the optimum implementation plan for revised CIP standards in this project.
- Address when newly identified critical assets or critical cyber assets, newly acquired equipment or assets, etc. must come into compliance with CIP standards.
- Address compliance issue where internal requirements exceed NERC requirements. Clarify in view of language contained in FERC Order 706 paragraph 377.

Clarify Existing Requirements

- Consider the need for different requirements for different environments e.g., control center, substation and generation plant.
- Clarify how serial and wireless devices are subject to these standards. Refer to pp 278 and 285 of FERC Order 706.

Other Issues

- Consider issues surrounding protection of data in motion.
- Consider the issue of hybrid devices that use both serial and routable protocols.
- Consider the issue of data versus information (electronic and/or hardcopy lists, drawings, etc.) protection including transport and transmittal of such information.

In this document comments have been organized so it is easier to interpret the comments. All comments received can be viewed in their original format at the following site:

http://www.nerc.com/~filez/standards/Project_2008-06_Cyber_Security.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

Individual or group.	Name	Organization	RBB Segment	
Individual	Thad Ness	AEP	5 - Electric Generators, 6 - Electicity Brokers, Aggregators , 1 - Transmission Owners, 3 - Load-serving Entities	
Individual	Gerald Freese	American Electric Power	3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators , 1 - Transmission Owners	
Individual	Jason Shaver	American Transmission Company	1 - Transmission Owners	
Individual	Paul Kerr	Coral Power, L.L.C.	6 - Electicity Brokers, Aggregators	
Individual	Kent Kujala	Detroit Edison	3 - Load-serving Entities, 5 - Electric Generators, 4 - Transmission-dependent Utilities	
Group	Louis Slade	Dominion Resources Services, Inc.	3 - Load-serving Entities, 6 - Electicity Brokers, Aggregators , 5 - Electric Generators	<table><tr><th></th><th>Additional Member</th><th>Additional Organization</th><th>Region</th><th>Segment Selection</th></tr><tr><td>1.</td><td>Harold Adams</td><td></td><td>RFC</td><td>3, 5, 6</td></tr><tr><td>2.</td><td>Jalal Babik</td><td></td><td>SERC</td><td>3, 5, 6</td></tr></table>
Individual	Greg Rowland	Duke Energy	1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators	
Group	Jack Cashin	Electric Power Supply Association	5 - Electric Generators	
Individual	Denise Roeder	ElectriCities of North Carolina, Inc.	6 - Electicity Brokers, Aggregators , 4 - Transmission-dependent Utilities, 3 - Load-serving	

<table>
<tr><th>Individual or group.</th><th>Name</th><th>Organization</th><th>RBB Segment</th><th></th></tr>
<tr><td></td><td></td><td></td><td>Entities</td><td></td></tr>
<tr><td>Group</td><td>Sam Ciccone</td><td>FirstEnergy Corp.</td><td>5 - Electric Generators, 6 - Electicity Brokers, Aggregators , 3 - Load-serving Entities, 1 - Transmission Owners</td><td></td></tr>
<tr><td>Individual</td><td>David Kiguel</td><td>Hydro One Networks Inc.</td><td>3 - Load-serving Entities, 1 - Transmission Owners</td><td></td></tr>
<tr><td>Individual</td><td>Ken Welch</td><td>LK4 Technology Corporation</td><td>Not Applicable</td><td></td></tr>
<tr><td>Group</td><td>Jason L. Marshall</td><td>Midwest ISO</td><td>2 - RTOs and ISOs</td><td>
<table>
<tr><th></th><th>Additional Member</th><th>Additional Organization</th><th>Region</th><th>Segment Selection</th></tr>
<tr><td>1.</td><td>Joe Knight</td><td>Great River Energy</td><td>MRO</td><td>1</td></tr>
<tr><td>2.</td><td>Kirit Shah</td><td>Ameren</td><td>SERC</td><td>1</td></tr>
<tr><td>3.</td><td>Joeseph DePoorter</td><td>Madison Gas and Electric Company</td><td>MRO</td><td>3, 4, 5, 6</td></tr>
</table>
</td></tr>
<tr><td>Individual</td><td>Martin R. Hopper</td><td>M-S-R Public Power Agency</td><td>9 - Federal, State, Provincial Regulatory, or other Government Entities</td><td></td></tr>
<tr><td>Group</td><td>Keith Stouffer</td><td>National Institute of Standards and Technology</td><td>9 - Federal, State, Provincial Regulatory, or other Government Entities</td><td>
<table>
<tr><th></th><th>Additional Member</th><th>Additional Organization</th><th>Region</th><th>Segment Selection</th></tr>
<tr><td>1.</td><td>Stu Katzke</td><td>NIST</td><td>NA - Not Applicable</td><td>9</td></tr>
<tr><td>2.</td><td>Marshall Abrams</td><td>Mitre</td><td>NA - Not Applicable</td><td>NA</td></tr>
</table>
</td></tr>
<tr><td>Group</td><td>Lee Pedowicz</td><td>NPCC</td><td>10 - Regional Reliability Organizations/Regional Entities</td><td>
<table>
<tr><th></th><th>Additional Member</th><th>Additional Organization</th><th>Region</th><th>Segment Selection</th></tr>
<tr><td>1.</td><td>Guy Zito</td><td>NPCC</td><td>NPCC</td><td>10</td></tr>
<tr><td>2.</td><td>Brian Hogue</td><td>NPCC</td><td>NPCC</td><td>10</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Individual or group.</th><th>Name</th><th>Organization</th><th>RBB Segment</th><th></th></tr>
<tr><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>3.</td><td>David Kiguel</td><td>Hydro One</td><td>NPCC</td><td>1, 3</td></tr>
<tr><td>4.</td><td>Kathleen Goodman</td><td>ISO New England</td><td>NPCC</td><td>2</td></tr>
<tr><td>5.</td><td>Ben Li</td><td>Independent Electricity System Operator</td><td>NPCC</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>Individual</td><td>George W. Brady</td><td>Ohio Valley Electric Corporation</td><td>1 - Transmission Owners</td><td></td></tr>
<tr><td>Individual</td><td>Greg Ward / Steve Martin</td><td>Oncor Electric Delivery Company LLC</td><td>1 - Transmission Owners</td><td></td></tr>
<tr><td>Individual</td><td>Ron Falsetti</td><td>Ontario IESO</td><td>2 - RTOs and ISOs</td><td></td></tr>
<tr><td>Group</td><td>Colin Anderson</td><td>Ontario Power Generation</td><td>5 - Electric Generators</td><td></td></tr>
<tr><td>Group</td><td>Robert Mathews</td><td>Pacific Gas and Electric Company</td><td>1 - Transmission Owners</td><td>
<table>
<tr><th></th><th>Additional Member</th><th>Additional Organization</th><th>Region</th><th>Segment Selection</th></tr>
<tr><td>1.</td><td>Dave Ambrose</td><td>WAPA - Loveland</td><td>WECC</td><td>1, 3</td></tr>
<tr><td>2.</td><td>Vern Kissner</td><td>Tacoma Power</td><td>WECC</td><td></td></tr>
<tr><td>3.</td><td>Marc DeNarie</td><td>WAPA - Folsom</td><td>WECC</td><td>1, 3</td></tr>
<tr><td>4.</td><td>Jeff Mantong</td><td>WAPA - Folsom</td><td>WECC</td><td>1, 3</td></tr>
<tr><td>5.</td><td>Gray Wright</td><td>Sierra Pacific Power</td><td>WECC</td><td>1, 3, 5</td></tr>
<tr><td>6.</td><td>Jamey Sample</td><td>CAISO</td><td>WECC</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>Individual</td><td>Todd Thompson</td><td>PJM Interconection</td><td>2 - RTOs and ISOs</td><td></td></tr>
<tr><td>Group</td><td>Annette Bannon</td><td>PPL Generation, LLC</td><td>5 - Electric Generators, 6 - Electicity Brokers, Aggregators</td><td>
<table>
<tr><th></th><th>Additional Member</th><th>Additional Organization</th><th>Region</th><th>Segment Selection</th></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Individual or group.</th><th>Name</th><th>Organization</th><th>RBB Segment</th><th></th></tr>
<tr><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>1.</td><td>Mark Heimbach</td><td>PPL EnergyPlus</td><td>RFC</td><td>6</td></tr>
<tr><td>2.</td><td>Mark Heimbach</td><td>PPL EnergyPlus</td><td>MRO</td><td>6</td></tr>
<tr><td>3.</td><td>Mark Heimbach</td><td>PPL EnergyPlus</td><td>NPCC</td><td>6</td></tr>
<tr><td>4.</td><td>Mark Heimbach</td><td>PPL EnergyPlus</td><td>SERC</td><td>6</td></tr>
<tr><td>5.</td><td>Mark Heimbach</td><td>PPL EnergyPlus</td><td>SPP</td><td>6</td></tr>
<tr><td>6.</td><td>Jim Batug</td><td>PPL Generation</td><td>RFC</td><td>5</td></tr>
<tr><td>7.</td><td>Jim Batug</td><td>PPL</td><td>NPCC</td><td>5</td></tr>
</table>
</td></tr>
<tr><td>Group</td><td>Phil Riley</td><td>Public Service Commission of South Carolina</td><td>9 - Federal, State, Provincial Regulatory, or other Government Entities</td><td></td></tr>
<tr><td>Individual</td><td>Daniel Hecht</td><td>Sempra Energy Trading LLC and Sempra Energy Solutions LLC</td><td>6 - Electicity Brokers, Aggregators</td><td></td></tr>
<tr><td>Group</td><td>Jim Busbi</td><td>Southern Company Services, Inc.</td><td>1 - Transmission Owners</td><td>
<table>
<tr><th>Additional Member</th><th>Additional Organization</th><th>Region</th><th>Segment Selection</th><th></th></tr>
<tr><td>1.</td><td>J. T. Wood</td><td>Southern Company Services, Inc.</td><td>SERC</td><td>1</td></tr>
<tr><td>2.</td><td>Roman Carter</td><td>Southern Company Services, Inc.</td><td>SERC</td><td>1</td></tr>
<tr><td>3.</td><td>Marc Butts</td><td>Southern Company</td><td>SERC</td><td>1</td></tr>
</table>
</td></tr>
</table>

Individual or group.	Name	Organization	RBB Segment	
				<table><tr><td></td><td></td><td>Services, Inc.</td><td></td><td></td></tr><tr><td>4.</td><td>Jay Cribb</td><td>Southern Company Services, Inc.</td><td>SERC</td><td>1</td></tr><tr><td>5.</td><td>Valerie Piazza</td><td>Southern Company Services, Inc.</td><td>SERC</td><td>1</td></tr></table>
Group	Charles Yeung	Southwest Power Pool	2 - RTOs and ISOs	
Individual	Eric Olson	Transmission Agency of Northern California	1 - Transmission Owners	
Individual	Michael Puscas	United Illuminating	1 - Transmission Owners, 3 - Load-serving Entities	
Individual	William Lucas	We Energies	3 - Load-serving Entities, 5 - Electric Generators	
Group	Robert Mathews - CIIMS Subcommittee Chair	WECC (Steve Rueckert)	10 - Regional Reliability Organizations/Regional Entities	
Group		WECC-NERC PMO - PacifiCorp	1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators	
Group	Patrick Miller	Western Electricity Coordinating Council	10 - Regional Reliability Organizations/Regional Entities	
Individual	Terri Eaton	Xcel Energy	1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators	

1. Do you agree with the scope of the proposed standards action?

Summary Consideration: Most of the commenters agreed that the scope of the standards action to address the items identified in the FERC Order 706 is appropriate. Some went on to suggest that a list of these items accompany the SAR to which the SAR DT agreed.

There were many comments objecting to the inclusion of Purchasing Selling Entities (PSE) as subject to the CIP-002 through CIP-009 Standards. The SAR DT agreed and removed PSE from the SAR.

In addition, several commenters suggested that the reference to the Functional Model is inappropriate because the Demand-side Aggregator identified in FERC Order 706 performs the same tasks as the Load-serving Entity – and the SAR already identifies the Load-serving Entity as a functional entity with responsibility for some of the requirements in the set of CIP standards. Consequently, the drafting team removed this reference in the revised SAR.

Organization	Question 1:	Question 1 Comments:
Xcel Energy	No	PSEs are involved in scheduling purchase and sales transactions between entities in the wholesale electric market. We are not aware of any activities undertaken by a PSE that could be manipulated from a cyber standpoint and result in compromising the integrity of the bulk electric system. We believe that NERC should be required to provide a credible justification for extending the reach of the CIP standards to PSEs. At this juncture, Xcel Energy does not believe that any such justification has been provided.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves more of an economic role, and less of a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
American Transmission Company	No	The SAR should be revised to include a list of all FERC issued directives including the identification of any specific due dates. This additional information will help the industry understand the amount of work the standards drafting team is being assigned. NERC likely has this information so the inclusion of the data should be simple.
Response: The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. The team disagrees that the intent of the list would be to either estimate the quantity or length of work to be performed or prioritize the work to be undertaken.		
NPCC	No	1. The SAR is not specific on which CIP standards are "low hanging fruit", which ones contain more contentious issues than the others. It does not identify a proposed implementation plan that would support multiple revisions

Organization	Question 1:	Question 1 Comments:
		to the standards, whereas some changes would be reviewed by industry, balloted, and submitted for approval. 2. The SAR indicates that if additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator--see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely directed ??that NERC should register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.? In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model as long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. In this case, we expect the "Demand Side Aggregator", which we believe performs the tasks listed under the LSE in the model, will register as an LSE. Hence, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this speculative revision to scope statement should be in the SAR. 3. The originating cause and this SAR's scope should not be limited to FERC Order 706. Experiences from stakeholder's implementing the Cyber Standards should be taken into consideration as lessons learned as part of the scope for developing Standards. Extending the SAR beyond FERC Order 706 should only be done if it will not affect timelines given by FERC. Also, interpretations made subsequent to the standards should be formally codified into the appropriate places in the standards, such as the CIP-006 interpretation and any FAQ interpretations.
Response: 1. The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. It is more appropriate that the SDT determine the timing and grouping of revisions to be submitted to industry for comment and ballot. 2. The SAR DT has removed references to the Functional Model from the revised SAR. 3. The SAR DT has added a list of stakeholder issues for the standard drafting team to address – and updating the FAQ document was added – as an issue for the SDT to address. These additional issues are aggregated into a supplementary SAR that will be posted for industry stakeholder review. The SAR DT modified the SAR to clarify that the interpretation of CIP-006-1 R1.1 shall be addressed.		
Southwest Power Pool	No	Comments: We generally agree with the scope of the SAR. However, we have the following clarifying questions/comments: The SAR should contain a complete, revised implementation plan for both current and proposed CIP implementation. The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator ? see Order 706 paragraph 51), which directly impact

Organization	Question 1:	Question 1 Comments:
		the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely directed [?.NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.]In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model for so long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. Hence, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this speculative revision to scope statement should be in the SAR.
Response: The STD will develop an implementation plan for the revised standards. The SAR DT acknowledges that the LSE is currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.		
Ontario IESO	No	1. The SAR is not specific on which CIP standards are "low hanging fruit", which ones contain more contentious issues than the others, and any proposed implementation plan that supports multiple revisions to the standards while some changes are reviewed by industry, balloted, and submitted for approval. 2. The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator ? see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely dircted [?.NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.] In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model for so long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. In this case, we expect the "Demand Side Aggregator", which we believe performs the tasks listed under the LSE in the model, will register as an LSE. Hence, we do not expect the functional model to be revised in order to address this directive. As a result, we do not agree that this speculative revision to the scope statement should be included in the SAR.
Response: **1.** The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. It is more appropriate that the SDT determine the timing and grouping of revisions to be submitted to industry for comment and ballot. **2.** The SAR DT acknowledges that the LSE is currently identified in the Functional Model as performing load shedding. The SAR DT has		

Organization	Question 1:	Question 1 Comments:
removed reference to Functional Model in the revised SAR.		
Hydro One Networks Inc.	No	(a) The SAR is not specific on which CIP standards contain more contentious issues than the others, and any proposed implementation plan that supports multiple revisions to the standards while some changes are reviewed by industry, balloted, and submitted for approval. (b) The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (e.g. Demand Side Aggregator ? see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. However, the FERC order has not asked NERC to revise its functional model; it merely directed NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk Power System. In our view, the "Demand Side Agregator" performs tasks that the FM lists under the LSE entity thus it should be registered as such. According to the above, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this revision to scope statement should be in the SAR.
Response: **1.** The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. It is more appropriate that the SDT determine the timing and grouping of revisions to be submitted to industry for comment and ballot. **2.** The SAR DT acknowledges that the LSE is currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.		
FirstEnergy Corp.	No	See our comments to the rest of the comment form, plus the following: 1. Although we agree the scope must address the FERC directed changes from Order 706, the SAR must be developed further and lay out a table of all the directives. We look at this first posting of the SAR as just a general starting point for the SAR drafting team who will further develop expectations for the standards drafting team. To aid the SAR drafting team and eventual standards development team, FE has tabulated the FERC directed changes in an Excel spreadsheet that we have submitted separately with these comments to NERC's Barbara Bogenrief. In addition, FE will provide more detailed guidance when the revised SAR is made available for comment. 2. It is not clear to FE how the FERC directed changes to the compliance elements such as Violation Factors and Violation Severity Levels will be handled by NERC staff or the eventual CIP standards drafting team. If they are to be addressed by the CIP standards drafting team, then changes to VRFs and VSLs should be included in the SAR scope.

Organization	Question 1:	Question 1 Comments:
Response: 1. The SAR DT thanks the commenter for the summary spreadsheet that accompanied his comments. The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. The drafting team prepared a similar document to the commenter's spreadsheet and it is Attachment #2 of the revised SAR. 2. The Standard Review guide (Attachment #1 of the SAR) that accompanied the posted SAR describes the scope of update work that all standards that come under revision must undergo. Included are the additions or revisions of Violation Risk Factors and Violation Severity Levels.		
Sempra Energy Trading LLC and Sempra Energy Solutions LLC	No	Sempra Energy Trading LLC and Sempra Energy Solutions LLC disagree with the proposed changes to the applicability section of the Cyber Security Standards (CIP Standards). The expansion of the CIP Standards? applicability to Purchasing-Selling Entities (PSEs) would result in the unnecessary imposition of the CIP Standards on pure power marketers, which are typically registered only as PSEs. The overarching purpose of the CIP Standards is the identification and protection of Critical Cyber Assets, which are those ? Cyber Assets essential to the reliable operation of Critical Assets.? (The Glossary of Terms Used in Reliability Standards, May 2, 2007 at 4 (Glossary) defines Cyber Assets as ?programmable electronic devices and communication networks including hardware, software, and data.?) Entities that do not own or operate any Critical Assets have no Critical Cyber Assets and, therefore, should not be required to comply with the CIP Standards. Pure power marketers engage in power purchase and sale transactions, but do not own or operate any physical electric generation, transmission, or distribution facilities. They also do not own or operate any Critical Assets, which by definition are physical facilities connected to or integrated with the grid. (The Glossary defines Critical Assets as ?facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.?) As a result, pure power marketers do not own or operate any Critical Cyber Assets and, therefore, should not be required to comply with the CIP Standards. Although power marketers may be users of third-party electronic systems (e.g., OASIS or scheduling systems) that may be considered Critical Cyber Assets, such access is limited to user functions and does not allow in any way marketers (or any other users) to control those Critical Cyber Assets or the underlying physical Critical Assets. Pure power marketers typically qualify and register only as PSEs. The proposed inclusion of PSEs in the applicability section of the CIP Standards would render the CIP Standards applicable to PSEs that are not also owners or operators of physical electric assets, such as power marketers. Such change would impose on such power marketers significant regulatory burdens and costs, without furthering the goals of the CIP Standards. Application of the CIP Standards should be limited to only those functional categories of entities that actually own or control physical electric assets that could be Critical Assets. Such entities are registered with NERC for the proper reliability function that results from the ownership or operation of physical electric assets (including Critical Assets), such as Generator Owner (GO), Generator Operator (GOP), Transmission Owner (TO), or Transmission Operator (TOP). To the extent GOs, GOPs, TOs, and TOPs are included in the applicability section of the CIP Standards, the current exclusion of PSEs from the CIP Standards does not result in any reliability gap, because

Organization	Question 1:	Question 1 Comments:
		owners or operators of Critical Cyber Assets are subject to the CIP Standards pursuant to the registration for the functions that relate to their ownership and operation of those physical assets. Indeed, if a power marketer contractually assumes responsibility for the reliability functions associated with the operation of a generator, that marketer will be required to add a GOP registration to its PSE registration. Thus, it appears that the only effect of revising the applicability section of the CIP Standards to include PSEs would be to impose on pure power marketers reliability standards that are not intended to apply to entities that do not own or operate any Critical Assets. The Commission has acknowledged that compliance with the CIP Standards may be difficult and burdensome and has provided for a three year phased implementation. Such burden should not be imposed on entities that do not own or operate Critical Assets and whose compliance with the CIP Standards would not further the reliability of the Bulk Electric System. In the alternative, if NERC revises the applicability section of the CIP Standards to include PSEs, it should qualify the term added in the applicability section to refer only to those PSEs that actually own or control physical electric assets. NERC has previously determined that it is in some cases appropriate to qualify the applicability of a standard to a functional category. For example, reliability standard PRC-016 applies to Transmission Owners, Generator Owners, and Distribution Providers, but its applicability is further limited to include only an entity ?that owns [a Special Protections System].? As a result, the standard does not apply broadly (and unnecessarily) to every Transmission Owner, Generator Owner, and Distribution Provider. NERC should similarly consider adequate qualifications in the applicability section of the CIP Standards that clearly limit the applicability of the CIP standards to only those PSEs that own or operate physical electric assets.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.		
Duke Energy	No	While we agree for the most part with the scope, the Critical Assets are generally Control Centers, Substations, and Critical Generation. What applicability does this standard have for LSE? Is it appropriate that LSE's are included?
Response: The SAR DT asserts that LSEs (especially with the capability of shedding load) may have significant effect upon the Bulk Electric System and therefore should be subject to these standards. The CIP-002-1 through CIP-009-1 Standards as currently approved contain requirements that apply to the Load Serving Entity.		
National Institute of Standards and Technology	No	NIST agrees with the proposed changes in FERC Order 706 and proposes several additional items for consideration listed in the comments section of Question 5 of this comment form.

Organization	Question 1:	Question 1 Comments:
Response: Thank you for your input. The SAR DT addresses your comments to question #5 below.		
Pacific Gas and Electric Company	No	Please see specific items in questions 2, 4, and 5.
Response: Please see the response to comments on questions 2, 4, and 5.		
Midwest ISO	No	See our answers to the other questions.
Response: Thanks for the input.		
M-S-R Public Power Agency	No	See Question 2 comments.
Response: See our Response to question #2.		
WECC (Steve Rueckert)	No	See specific items in questions 2, 4 & 5
Response: See our Responses to question #2, 4 and 5.		
Ohio Valley Electric Corporation	No	
Oncor Electric Delivery Company LLC	No	
WECC-NERC PMO - PacifiCorp	Yes	Specifically, the scope needs to assure that the NIST standards are considered. Such standards will hlep organizations overcome confusion where elements of the existing standard is unclear.
Response: The SAR DT agrees. Order 706 directs consideration of NIST standards.		
Ontario Power Generation	Yes	see comments below
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
Coral Power,	Yes	Assuming the question should read: "Do you agree with the scope of the proposed standards action ?" The

Organization	Question 1:	Question 1 Comments:
L.L.C.		scope of the SAR is reasonable, since it is to address the directives of Order 706. Yet, this needs to be differentiated from the proposal in the SAR to expand the scope of applicable entities to include the Regional Entity and Purchasing-selling Entity. Inclusion of PSEs was not directed in the Order, or even considered as part of the NOPR, and should be removed from the SAR.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
We Energies	Yes	We Energies feels that incorporating the FERC 706 directives will privide additional clarity around implementation requirements and compliance measures to the existing CIP 002-009 standards.
Response: Thank you for your input.		
Electric Power Supply Association	Yes	Yes. To the extent that the proposed SAR incorporates actions identified in FERC Order 706, the scope is appropriate. Given the recent, very thorough vetting of this issue through the FERC NOPR and Order process, the Standards Drafting Team should be very cautious about any extensions to that scope.
Response: The SAR DT thanks the commenter for its input. Extensions to the scope will be determined by industry input as submitted to question #5 and #6.		
ElectriCities of North Carolina, Inc.	Yes	However, do not agree with expanding the scope of applicability as stated (see **Response** to Q2).
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
Southern Company Services, Inc.	Yes	Please see our comment to Question #2.
Response: Please refer to our Response to Question #2		
LK4 Technology Corporation	Yes	The industry needs to adopt a common risk assessment methodology. As a veteran compliance auditor for FFIEC, GLBA and SarBox, I have seen entire compliance programs disallowed because they did not start with

Organization	Question 1:	Question 1 Comments:
		the risk assessment. The NRC recently commissioned a cybersecurity risk assessment program and is in the process of commissioning a physical risk assessment. These risk assessments can be personalized for each individual complying entity, but a core criteria must be met by all.
Response: Thank you for your input. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available.		
PJM Interconection	Yes	
Detroit Edison	Yes	
PPL Generation, LLC	Yes	
American Electric Power	Yes	
United Illuminating	Yes	
AEP	Yes	
Western Electricity Coordinating Council	Yes	
Dominion Resources Services, Inc.	Yes	
Public Service Commission of South Carolina	Yes	

2. This SAR proposes to add the Regional Entities and Purchasing-Selling Entity functions to the applicability section of the revised standards. If additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria) as a direct result of Order 706 (i.e., Demand Side Aggregator — see Order 706 paragraph 51), which directly impact the applicable functions, conforming modifications will be made to the cyber security standards. Do you agree with these proposed changes to the applicability sections of these standards?

Summary Consideration: Nearly all the respondents believed that Purchasing Selling Entities should not be subject to the Cyber Security standards. The SAR DT agrees and has removed PSEs from the applicability section of the revised SAR. Several commenters indicated that the reference to the Functional Model should be removed because the FERC Order did not reference the Functional Model and because the tasks assigned to the Demand Side Aggregator are performed by the Load-serving Entity. The drafting team agrees that the tasks assigned to the Demand Side Aggregator are performed by the Load-serving Entity, and the reference in the SAR to the Functional Model modifications has been removed. The SAR already identifies the Load-serving Entity as having responsibilities for some requirements in CIP-002-1 through CIP-009-1.

Organization	Question 2:	Question 2 Comments:
Xcel Energy	No	As noted above, we do not believe that any justification has been provided for extending the reach of the CIP standards to PSEs.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
Ontario Power Generation	No	I see no need to expand the applicability of the CIP Standards to PSEs. This appears to be an indirect method of including market data - a subject that was contemplated within FERC's NOPR and widely opposed.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
PPL Generation, LLC	No	PPL Supply disagrees with the intent to add the PSE funtion to the CIP applicability. It is not clear to PPL how the transactions by a PSE would involve critical cyber assets essential to the reliable operations of the BPS.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place.		

Organization	Question 2:	Question 2 Comments:
Therefore the PSE is removed form the SAR as an applicable entity.		
Pacific Gas and Electric Company	No	Paragraph 4 of the SAR isn't clear. Assuming that the proposal of this paragraph, and it's bullets, is directly related to FERC Order 706 Paragraph 272, we would recommend rewording to:"This SAR will provide clairty in identifing various types of assets that feed information to critical assets used to support the reliability and operability of the Bulk-Power System as directed in FERC Order 706 Paragraph 272. This includes how to addess: - Regional Entities and Purchasing-Selling Entity functions as they relate to the reliability and operability of the Bulk-Power System. - Reliability and Market Interface Principle 4 (plans for emergency operations and system restoration).
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. The Regional Entities are subject to standards through the Delegation Agreements with NERC.		
Coral Power, L.L.C.	No	Making the standards applicable to the Regional Entity function was in the NOPR, commented on by stakeholders, considered by FERC and determined to be appropriate (paragraph 47). A great deal of discussion and consideration went to addressing comments and concerns regarding demand side aggregators, concluding with the direction that NERC should consider whether there is a need to register such entities and, if so, to address related issues and develop criteria for their registration (paragraph 51). As such, it is easy to agree that the applicability sections of the standards should be changed in line with the Order. However, nowhere, in this Order or in the NOPR, did FERC propose or contemplate or even discuss the inclusion of PSEs as responsible entities for the CIP standards. If there were any concerns related to PSEs they would have been raised by FERC and/or pursued by stakeholders, similar to those regarding small entities. FERC considered this, and determined that it would be "overly-expansive" to require every entity connected to the Bulk-Power System, to comply with the CIP standards, regardless of size (paragraph 49). PSEs, of course, are not even connected to the BPS.In reaffirming its reliance on the NERC registration process to identify entities that should comply with the CIP standards, FERC was not directing NERC to go back and make them apply to more entities, like PSEs. On the contrary, in listing all of the responsible entities that must comply with the CIP standards in paragraph 31, it is clear that FERC knew exactly which entities the standards do not - and should not - apply to. There is no explanation or support within the SAR describing the logic or reliability reasons for making PSEs responsible entities under the CIP standards. The only justification appears to be the desire to address the directives of FERC in Order 706, but there is no such directive to include PSEs. The SAR should be amended to eliminate the expansion of the applicability to PSEs.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and		

Organization	Question 2:	Question 2 Comments:
equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
AEP	No	In general a PSE has no direct control on system (e.g. OASIS, organized Market Applications) and/or the grid, and relevant transactions are ultimately approved or denied by a current reliability function such as the Interchange Authority, Balancing Authority and Reliability Coordinator. The PSE function was originally (and still is) designed in the context of the physical scheduling process to assign financial responsibility in the related contract path represented on an eTAG.A PSE neither creates load or generation, and at all times only serves as an intermediary, in a bilateral transaction, to schedule generation to load.There is already enormous confusion as to what an LSE does (Market based functions vs. Reliability based functions), and in reality, what FERC references in Order 706 best aligns with the LSE function, definitely not a PSE function, so lets not further confuse the issue by wrongly including the PSE function in this debate.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
ElectriCities of North Carolina, Inc.	No	By definition, the PSE purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. To accomplish that, it would have to work through other entities (TSPs, BAs, TOPs, GOPs, etc.) that are already required to meet the cyber security standards and that DO have responsibilities for managing and operating the facilities and processes that actually impact the reliability of the BES. If the PSE happens to be an affiliated merchant or a generator owner itself, then in addition to being registered as a PSE, that entity should also be registered according to the other functions it performs and would have to comply with the cyber security standards on those registration bases. It does not make sense to extend registration to PSEs, or any other functional entity, whose function itself does not physically impact the reliability of the BES.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
Ontario IESO	No	We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling

Organization	Question 2:	Question 2 Comments:
		Entities. Regional Reliability Organizations were included as applicable entities in the previously submitted CIP standards; the proposal to include the RE is a only matter of name change with respect to the revised Functional Model. However, we do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order. With respect to the proposal to make conforming changes to the cyber security standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see our comments on Q1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.		
Hydro One Networks Inc.	No	(a) We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling Entities. However, clarification must be sought from FERC because Regional Entities are not Owners, Users or Operators of the BPS, thus not legally subject to reliability standards (b) We do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities and we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order. (c) With respect to the proposal to make conforming changes to the CIP standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see our comments in Question 1. Furthermore, we do not agree with the need to change reliability standards if the Compliance

Organization	Question 2:	Question 2 Comments:
		Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We do not believe that changes the Compliance Registration Criteria would trigger a need to change the standards.
Response: a. The Regional Entities are subject to standards through the Delegation Agreements with NERC. b. The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. c. Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.		
NPCC	No	The SAR should remove the applicability to the RE. The RE is not a user owner or operator and does not have Critical Cyber Assets that control the BPS. We do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order. With respect to the proposed to make conforming changes to the cyber security standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please refer to the comments above in Question 1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The Regional Entities do have an “impact on the operation of facilities, systems and equipment. . .” and are subject to standards through the		

Organization	Question 2:	Question 2 Comments:
Delegation Agreements with NERC. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.		
Ohio Valley Electric Corporation	No	Regional Entities are not users, owners or operators of the Bulk Electric System and thus the reliability standards do not apply to them by definition. It is not clear why the LSE and PSE are to be included. LSEs and PSEs do not own any Critical Assests that directly affect the bulk electric system. Subsequently, these entities could not have any Critical Cyber Assets.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The Regional Entities do have an "impact on the operation of facilities, systems and equipment. . ." and are subject to standards through the Delegation Agreements with NERC. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. Load-serving Entities are already identified as a responsible entity for requirements in CIP-002-1 through CIP-009-1.		
Midwest ISO	No	Regional Entities are not users, owners or operators of the Bulk Electric System. Thus, reliability standards can't apply to them by statute. It is not clear why the LSE and PSE are included. The LSE and PSE will not own any Cyber Assets that directly affect Critical Assets. Thus, it is not possible for them to have Critical Cyber Assets.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The Regional Entities do have an "impact on the operation of facilities, systems and equipment. . ." and are subject to standards through the Delegation Agreements with NERC. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		

Organization	Question 2:	Question 2 Comments:
Load-serving Entities are already identified as a responsible entity for requirements in CIP-002-1 through CIP-009-1.		
Dominion Resources Services, Inc.	No	The FERC order stated "that demand side aggregators might also need to be included in the NERC registration process if their load shedding capacity would affect the reliability or operability of the Bulk-Power System. The current version of NERC functional model definition of PSE does not contain any reference to load shed capability, which is the focus of FERC's comment. As we've stated in comments to other standards, the ability to shed load lies with the asset owner of the physical infrastructure.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
Oncor Electric Delivery Company LLC	No	Oncor Electric Delivery does not agree that the Demand Side Aggregator should be a registered Entity subject to the NERC CIP standard. For purposes of Load Shedding within ERCOT, Oncor Electric Delivery performs this function as directed in ERCOT's Guides and Protocols.
Response: The SAR DT acknowledges that the LSEs are currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.		
Electric Power Supply Association	No	No. The SAR notes that based on a previous SAR, finalized on March 8, 2004, they intend to expand the applicability to include PSEs. EPSA does not agree with this addition. FERC Order 706 makes no suggestion that such an expansion of the applicability is appropriate. Indeed in Paragraph 31 of the Order, they note the 11 Functional Model entities that they believe are covered by the Order and PSEs are not included. If there was an intent to expand the applicability of the Standards, based on a 2004 SAR, it would have been appropriate to raise that issue during the FERC procedure.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
M-S-R Public Power Agency	No	M-S-R Public Power Agency ("M-S-R") has determined that the SAR's proposal to add Purchasing-Selling Entities ("PSE") to the applicability section of the revised standards is out of scope and inappropriate.NERC's announcement for this comment period states that "The SAR proposes to bring the following standards (i.e. CIP-

Organization	Question 2:	Question 2 Comments:
		002-1 through CIP-009-1) into conformance with the ERO Rules of Procedure and to address the directives from FERC Order 706," but our review of these documents finds no suggestions, let alone directives, indicating that these standards should become applicable to PSE. In Order 706 at Paragraph 49, FERC cautions against an "overly-expansive" approach "requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry."M-S-R contends that the PSE function in and of itself does not involve any Critical Assets, let alone Critical Cyber Assets and therefore concludes that the proposed PSE applicability of the revised standards is inappropriate. In its "Glossary of Terms Used in Reliability Standards" as adopted by the NERC Board of Trustees on February 12, 2008, NERC provides the following definitions of terms essential to the applicability of the CIP standards:Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.While an entity's business practices related to the PSE function may involve confidential information related to power contracts and prices and this information may be resident on Cyber Assets, there is no manner in which these assets could affect the reliability or operability of the Bulk Electric System if destroyed, degraded, or otherwise rendered unavailable. Adding PSE to the applicability section of the revised standards would cause every entity registered as a PSE to comply with the requirements of CIP-002 only to annually confirm that it has no Critical Cyber Assets. Such an exercise would be unnecessarily burdensome to entities that are already incurring high costs to comply with the appropriately applicable standards.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
WECC (Steve Rueckert)	No	Paragraph 4 of the Detailed Description section in the SAR isn't clear. Assuming that the intent of this paragraph is directly related to FERC Order 706 Paragraph 272, recommend revising the section to reflect that the scope of the drafting effort:? Provide clarity in identifying various types of assets that feed information to critical assets used to support the reliability and operability of the Bulk-Power System as directed in FERC Order 706 Paragraph 272. This includes how to address: - Regional Entities and Purchasing-Selling Entity functions as they relate to the reliability and operability of the Bulk-Power System. - Reliability and Market Interface Principle 4 (plans for emergency operations and system restoration).?
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of		

Organization	Question 2:	Question 2 Comments:
such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. The Regional Entities are subject to standards through the Delegation Agreements with NERC.		
Southwest Power Pool	No	Comments: We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling Entities. Regional Reliability Organizations were included as applicable entities in previously submitted CIP standards; the proposal to include the RE is a matter of name change. However, we do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on Critical Assets, nor can we find its inclusion stipulated in the FERC Order. Wrt the proposed to make conforming changes to the cyber security standards if additional e our comments on Q1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.		
Sempra Energy Trading LLC and Sempra Energy Solutions LLC	No	See answer to Question 1
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of		

Organization	Question 2:	Question 2 Comments:
such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
Southern Company Services, Inc.	Yes	We agree with the RE and PSE additions if it makes sense. However, if the drafting team feels that this is not appropriate remove it As to the DSM function, it appears that this is just a subset of the LSE function and this is just a market function. The drafting team should consider if this is a duplicative function of the LSE.
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity. The Regional Entities are subject to standards through the Delegation Agreements with NERC. The SAR DT acknowledges that the LSEs are currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.		
LK4 Technology Corporation	Yes	A cyber security system is only as strong as its weakest link. Having unaudited systems interfacing with complying systems represents a large identifiable risk.
Response: The SAR DT thanks you for your comment. The standards CIP-005 and CIP -007 address the types of issues you refer to in your comment. Use of an electronic security perimeter (ESP) implies a mutual distrust posture that requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an ESP regardless of where that communication originates.		
FirstEnergy Corp.	Yes	The CIP standards should be adjusted to cover any and all functional entities that can impact the reliable operations of the BES. The CIP standards should be adjusted to focus on entities who own cyber entry points that can lead to a compromised BES. Presently the CIP-002 standard is focused on identification of critical BES assets (transmission/generation) and then reviewing those assets for critical cyber assets. This approach could exclude functional entities that do not own BES assets but have an impact on the reliable operation of BES assets.
Response: The SAR DT thanks you for your input. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available. Applicability of the CIP Standards to any entity with cyber entry points as a criterion for who should be subject to these requirements has merit. Attachment #1 of the SAR allows for review of the Applicability section of these standards to ensure there are no overlaps or gaps.		
PJM Interconection	Yes	

Organization	Question 2:	Question 2 Comments:
Detroit Edison	Yes	
American Transmission Company	Yes	
American Electric Power	Yes	
United Illuminating	Yes	
National Institute of Standards and Technology	Yes	
We Energies	Yes	
Western Electricity Coordinating Council	Yes	
Duke Energy	Yes	
Public Service Commission of South Carolina	Yes	

3. If you are aware of any regional variances or associated business practices that we should consider with this SAR please identify them here.

Summary Consideration: None of the commenters are aware of any regional variances or associated business practices as they pertain to Cyber Security. The SAR DT agrees that there should be uniform technical requirements and consistent auditing of these requirements across regions.

Organization	Regional Variance	Business Practice:
Xcel Energy	As noted above, the rationale for applying the CIP standards to PSEs has not been provided. Absent an understanding of the reasons for pulling PSEs within the ambit of the CIP standards, we are unable to comment on the need for any regional or business practice variance.	
Response: The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.		
PJM Interconection	Regional variances should be few if any. The Regional Entities will need to apply compliance guidelines consistently across the U.S. in order to circumvent issues with inconsistency.	
Response: The SAR DT thanks you for your input with respect to regional variances. The team asserts that there should be uniform technical requirements and consistent auditing of these requirements across regions.		
American Transmission Company	ATC is not aware of any regional or business variance that the SDT should consider.	
We Energies	We Energies is not aware of any regional or business variance that the standards team should consider.	
Southern Company Services, Inc.	We know of no regional variances to identify at this point. However, if at some point in time the drafting team feels one is necessary they should consider adding it.	
Pacific Gas and Electric Company	None	
M-S-R Public Power Agency	None.	
WECC (Steve Rueckert)	none	

4. Do you agree with the "multi-phase" approach identified in the SAR? (The SAR's proposal is to take the easiest modifications through the posting and balloting cycles first, followed by one or more sets of modifications to address those directives that will take more time.)

Summary Consideration: The comments ranged from agreement with to cautious opposition to a "multi-phase" approach to this project. The SAR DT believes that the SDT ought to adopt the optimal approach on their own accord as they will be in the best position to determine work approach. Therefore the SAR will not constrain the SDT to adopting a multi-phase approach but instead provide the SDT the latitude to choose one in order to accomplish the objectives set forth in the SAR.

Organization	Question 4:	Question 4 Comments:
Xcel Energy	No	Any further changes to the CIP standards should be proposed and adopted on a comprehensive basis. The piecemeal approach contemplated in this question creates a significant risk that changes adopted in one cycle could be altered or overridden by changes approved in a subsequent cycle, undermining the ability of stakeholders to efficiently and effectively manage costs of implementing the CIP standards. The industry is engaged in a very substantial effort to ramp up to comply with the existing standards. This effort will result in substantial additional costs to companies and consumers. While this effort is ongoing, the CIP landscape is continuing to change, creating the very real possibility that work that is currently ongoing will become obsolete with the next round of CIP standards. The current situation will only be exacerbated if the next phase of the CIP standards are adopted on a piecemeal basis.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Detroit Edison	No	A "multi-phase" approach is a sound idea for a task of this magnitude however, the order of modifications should be based on priority rather than ease of implementation. FERC Order 706 clearly stated that "Reasonable Business Judgment" (P138) and "Acceptance of Risk" (P150) need to be removed and "Technical Feasibility" exceptions need to have criteria developed to ensure accountability (P222). The first two would most likely fall into the easy category and the third might not. The "Technical Feasibility" language used by FERC indicates that it should be high on the priority list and should not be delayed because it may be difficult to address. Other high priority issues should include Periodic Self Certifications (P96). The drafting team should consider all of FERC's comments, determine priorities, and plan a revision schedule based on those priorities
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		

Organization	Question 4:	Question 4 Comments:
Ontario Power Generation	No	The multi-phase approach appears cumbersome and confusing. The standards will be in a perpetual state of flux and members will have a more difficult time implementing programs to ensure compliance against a moving target. Modifications should be done in a comprehensive fashion.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Ohio Valley Electric Corporation	No	Registered entities have already been working towards compliance with the CIP standards per the existing implementation plan. The drafting team is now proposing to make changes before the existing implementation plan is complete. Registered entities need to be allowed to become compliant with the existing standards before additional changes are made to the CIP standards. Otherwise, the drafting team is creating a moving target that provides an incentive to delay implementation right up until an entity is required to be auditably compliant. By delaying their implementation, registered entities could save costs from having to make multiple changes to meet changing CIP requirements without incurring penalites. FERC confirmed in Order 706 that no penalties could be applied until the auditably compliant phase.The drafting team should list the required changes from FERC Order 706 directly in the SAR and what class they consider the change to be in. Also, if additional and acceptable changes are requested from the commentors, these changes should be listed in the SAR and clearly marked as coming from industry.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
PPL Generation, LLC	No	PPL Supply disagrees with the SDT's approach to addressing issues through multiple revisions. This approach will add complexity and rapid changes to the standards making it difficult for entities dealing with implementing plans, some with long lead-times, to be compliant with the changing requirements.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Pacific Gas and Electric Company	No	In theory it is a reasonable approach if the first phase only consist of simple changes to reporting timeframes, etc. that don't have any interrelation or complexity to controveral topics. Then phase two be addressed as a whole versus multiple interations. This is because we feel that multiple interations will only increase the oveall administrative burden on the drafting team, increase complexity of an already complex task, possibably result in throw awary work, and impact our ability to deliver a cohesive, quality, and timely product.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be		

Organization	Question 4:	Question 4 Comments:
submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
NPCC	No	While we support this as a general approach when NERC develops several standards at the same time, we are unable to further comment on its merit absent any proposed implementaiton plan and any indication in the SAR as to which standards are "low fruit dropping" and which ones are more controversial than the others. We would suggest, however, that the inter-relationship among these standards be considered in developing the staged implementation plan. We recommend that the SAR be broken into two or more SARs. The first SAR can address the "low hanging," less contentious issues. A second SAR can address the more contentious issues.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Midwest ISO	No	Registered entities have already been working towards compliance with the CIP standards per the existing implementation plan. Now, this drafting team is proposing to make changes before the existing implementation plan is complete. Registered entities need to be allowed to become compliant to the existing standards. Afterward, then additional changes can be made to the CIP standards. Otherwise, the drafting team is creating a moving target that provides an incentive to delay implementation right up until an entity is required to be auditably compliant. By delaying their implementation, registered entities could save costs from having to make multiple changes to meet changing CIP requirements without incurring penalites. FERC confirmed in order 706 that no penalties could be applied until the auditably compliant phase. We also believe that the drafting team should list the required changes from FERC Order 706 directly in the SAR and what class they consider the change to be in (i.e. low hanging fruit ,etc.) Also, if additional acceptable changes are requested from the commenters, these changes should be listed in the SAR and clearly marked as coming from industry.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Duke Energy	No	We are concerned about how "easy" versus "contensious" issues will be identified. Furthermore a staggered approach will add complexity to corresponding changes that must be made to the implementation plan. The SDT should consider getting all changes in one revision to simplify the process.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Ontario IESO	No	We do not agree with the "multi-phase" approach. Such an approach brings out multiple concerns - which set of standards should we begin to focus our attention on while developing implementation plans as these cannot be

Organization	Question 4:	Question 4 Comments:
		developed and implemented overnight - what if we or any other applicable entity begin work on a set of standards which ultimately gets voted down by the industry - should we wait to see which set of standards gets the assent which would mean delays in the implementation phases - what factors decide which set of standards go through - would this not bring into the forefront issues related to costs and risk mitigation. There are too many questions that would remain if such an approach were to be applied. We strongly suggest that all these standards be developed and implemented at the same time to avoid confusion. If it becomes necessary to implement these standards in stages, we urge the SDT to consider the inter-relationship among these standards and clearly convey the rationale for a staged implementation plan.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
FirstEnergy Corp.	Yes	Regarding the "multi-phase" approach and going after the "low hanging fruit" first, while that may be prudent, it is also important to quickly focus on modifications to CIP-002 since it drives all other CIP requirements. Also, by changing CIP-002 first, the "critical asset list" will be focused solely on whether there is a true belief of BES criticality rather than be influenced by what an organization may have to do to secure the assets.The team should consider three phases:Phase 1: Handle the "urgent" issues for specific changes and timelines as directed by FERC (such as the removal of "reasonable business judgment" phrase from the standards). These could even be handled through separate "Urgent Action" SAR/Standard revisions as allowed by the NERC standard development process.Phase 2: Properly develop CIP-002 since this standard lays the groundwork for the other 7 CIP standards.Phase 3: Develop the rest of the requirements to CIP-003 through CIP-009 per the FERC directed modifications.
The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior such as your proposed three phases, it has the latitude to proceed as such.		
Hydro One Networks Inc.	No	While this might be an acceptable approach, we are unable to further comment on its merit absent any proposed implementaiton plan and any indication in the SAR as to which standards are "low hanging fruit" and which ones are more controversial than the others. We would suggest, however, that inter-relationship among these standards be considered in developing the staged implementation plan.Alternatively, the SAR could be broken into several SARs one for each phase.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Southwest Power	No	Comments: We do not agree with the multi-phased approach to implementation. The industryis already

Organization	Question 4:	Question 4 Comments:
Pool		implementing the current CIP standards in a phased approach, implementing another series of revised standards in the same manner would only cause confusion as to which standards are applicable when and what is required. This approach also creates an incentive to wait as long a possible to become compliant. If a registered entity commits assets today to become compliant, it may have to commit more later to make modifications to meet the changes to the standards. However, if the registered entity waits until later phases of the implementation plan, it may commit less assets overall since it may avoid multiple investments. As long it complies by the auditably compliant phase, then they cannot be fined for non-compliance, per FERC Order 706.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
M-S-R Public Power Agency	No	M-S-R cannot agree with the "multi-phase" approach without knowing how the "easiest modifications" have been or will be identified. If adding PSE to the applicability section of the revised standards has been or could be considered an easy modification, then M-S-R is opposed to the "multi-phase" approach.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
WECC (Steve Rueckert)	No	In theory, it is a reasonable approach if the first phase only consist of simple changes to reporting timeframes, etc. that don't have significant interrelation, complexity or controversial topics. Then phase two be addressed as a whole versus multiple iterations. This is because we feel that multiple iterations will only increase the overall administrative burden, increase complexity of an already complex task, possibly result in throw away work, and impact the ability to deliver a cohesive, quality, and timely product
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
American Transmission Company	Yes	Including a list of all FERC order directives will aid that industry and the SDT to efficiently organize the multiple phases.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
American Electric Power	Yes	Logical progression.

Organization	Question 4:	Question 4 Comments:
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
PJM Interconection	Yes	
Southern Company Services, Inc.	Yes	It is our understanding that the SAR drafting team will consider the directives from the FERC order first and establish a priority level. The less contentious and less complicated items are assumed to be considered first for quick turnaround, followed by the more difficult issues.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
AEP	Yes	It should be well established that the standards revisions are not to be construed as standards re-writing. The basic concepts except as noted by FERC in the final rule should stand.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
We Energies	Yes	We Energies would like to see the drafting team address modifications as they apply to any requirement(s) throughout the standard set.
Response: Note that the Attachment #1 of the SAR includes reviewing each of the standards to ensure that it conforms to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure as outlined in the Standard Review Guidelines		
Western Electricity Coordinating Council	Yes	This may be more difficult than it seems, but the approach is a good idea and should be allowed. There may be issues that seem easier than others at the onset of the effort which could ultimately end up being far more contentious than originally expected. Greater success may be found if there is a defined process for flexibility around these unforeseen challenges such as a transition mechanism from the "easy" to "hard" range.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
ElectriCities of North Carolina, Inc.	Yes	As long as it is perfectly clear to all stakeholders at any time which modifications are under review, which are being balloted, and which are being submitted for approval.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be		

Organization	Question 4:	Question 4 Comments:
submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
LK4 Technology Corporation	Yes	However, adoption/adaptation of the FFIEC could be a model to speed the phases. The underlying ISO requirements are identical.
Response: The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Coral Power, L.L.C.	Yes	
United Illuminating	Yes	
National Institute of Standards and Technology	Yes	
Dominion Resources Services, Inc.	Yes	
Public Service Commission of South Carolina	Yes	
Oncor Electric Delivery Company LLC	Yes	
Electric Power Supply Association	Yes	

5. Based on the limited experience of implementing the current standards, are there any other issues that are not addressed in Order 706 that should be changed?

Summary Consideration: Many commenters identified issues in addition to the directives and recommendations contained in the Order 706. The SAR DT found some to have merit and added these to the SAR as Attachment 3. The additional issues include the following:

- the SDT to develop additional implementation plans as part of their work scope
- address a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means
- consider the issue of implementing these standards in the substation and generating environment
- consider modifying the standards to clarify the issue of hybrid devices that use both serial and routable protocols
- consider how to provide additional guidance on control centers in support of these standards

Other comments emphasized particular Order 706 directives and recommendations such as coordination with and consideration of other cyber-related standards, guidelines and activities. These items are explicitly listed in the revised SAR, e.g., confer with NRC and others with respect to Nuclear facility exemption.

Organization	Question 5:	Question 5 Comments:
Xcel Energy	Yes	First, we believe that a shift in the approach to development of the CIP standards is needed. We believe that the standards need to be redirected toward performance-based expectations rather than command and control directives. The command and control approach currently embodied in the standards is too rigid and inflexible in a rapidly changing environment to effectively and efficiently protect grid assets from cyber threats that may develop in the coming years. A more performance-based approach would allow industry the flexibility to adjust to a rapidly changing environment in the most efficient and effective manner. In addition, an overall goal or mission statement for the CIP process should be established that clearly identifies the objectives of the standards. Presently, we believe that the distinction between cyber security (which we understand to be the objective of the standards) and physical security is not being effectively maintained in the standards. Clarity about the objective of the CIP standards should help ensure a more clear and precise set of changes to the standards.
Response: Thank you for the input. The NERC Standards are performance-based as a guiding principle. All standards shall have a clear reliability objective. In Attachment 1 to the SAR, there is an outline of the modifications that will be made to the set of standards, and bringing additional clarity to the requirements is one of the objectives the standard drafting team will try to achieve. With respect to the separation of physical security from cyber security, the family of standards of which these are a part pertain to critical infrastructure protection. These 8 standards pertain to cyber security of which one component is the physical security of those assets.		
American	Yes	The SDT should develop a standard timeline for a newly identified Critical Asset to reach compliance. Any newly

Organization	Question 5:	Question 5 Comments:
Transmission Company		identified Critical Asset will take a considerable amount of time for an entity to become fully compliant with the CIP Standards (CIP-002 - 009). This is not included in the existing CIP standards but we believe that it is something that should be addressed in the phase of standards development. Also, by including a list of all FERC ordered directives in the SAR that SDT will be able to determine when it's best to address these other suggested changes.
Response: We agree and thank you for your input. Your suggestion to develop a standard timeline for a newly identified Critical Asset to reach compliance is included in list of added stakeholder issues for the standard drafting team to address. These additional issues are aggregated into Attachment 3 in the revised SAR. A list of the FERC directives has also been added to the revised SAR as Attachment #2.		
PPL Generation, LLC	Yes	The Rev. 1 CIP-007, 008, and 009 standard requirements are largely consistent with the Control Center/SCADA/EMS operating environment. The requirements of these standards are new to generating plant and substation environments. The project should better address the application of CIP-005, CIP-007, CIP-008, and CIP-009 to generation plants and substations, and if appropriate include development of guidance or reference to NIST SP800 series reports.
Response: The SAR DT acknowledges that the substation environment is gradually becoming comparable in terms of cyber security importance with control center environments. The following issues have been added to Attachment 3 in the revised SAR: 1. Consider the unique issues of implementing these standards to the substation and generating environment sub station considerations is among these issues. 2. Consider how to provide additional guidance on control centers in support of these standards.		
Pacific Gas and Electric Company	Yes	In general the industry seems to still be challenged in situations where there are hybrid devices that use both serial and routable protocols. An example is where a Critical Cyber Asset is a serial device which is connected directly to a router, thus converting it to a routable protocol. The SAR should include explicity address these types of situations. We are not recommending that we expand the current CIP scope to include serial devices, but rather explicit guidance.
Response: The SAR DT thanks the commenter for the input. The SAR DT has added a list of stakeholder issues for the standard drafting team to address – and hybrid devices is among those issues. The following issue has been added to Attachment 3 in the revised SAR: ▪ Consider modifying the standard to clarify the issue of hybrid devices that use both serial and routable protocols.		
National Institute of Standards and Technology	Yes	General Comments Summary: NIST believes that if the changes specified in FERC Order 706 and the recommendations below are implemented, NERC will have made a positive step towards making the CIPs commensurate with the NIST SP

Organization	Question 5:	Question 5 Comments:
		800-53, Rev 2 moderate baseline. However, there are still differences in coverage and in the level of specificity of the security requirements that need to be addressed. NIST would also like to point out that many of the federal agencies that own/operate industrial control systems in the bulk electric sector are classifying their systems as High impact systems that implement the High baseline requirements in SP 800-53.NIST is willing and has the resources to work on the NERC standards team in developing the next revision to the standard. Approach: Critical Assets vs. Information System - NIST understands that in the electric sector, protecting critical assets has been the predominant paradigm, but recommends for future revisions of the standards that an information systems approach rather than critical asset approach be considered. Our rationale for this suggestion is as follows: While it is important to identify critical assets using a risk-based assessment methodology, NIST suggests that NERC consider applicability of the CIPs at an information system level rather than at the critical asset level. An information system view provides a more natural context for the application of information technology security across an industrial control system composed of multiple components, where some subset of the components is supported by information technology. Under the current scope of the CIPs, all of the CIP security requirements would be applied to every critical cyber asset. In some cases, application of all of the CIP security requirements to a critical cyber asset may not make sense or may be excessive due to the nature of the asset. When an information system view is adopted, the CIP security requirements would be applied at the information system level, resulting in the allocation of CIP requirements to specific components. All components of the information system are not required to support every information system security requirement? just those that are identified as a result of the requirement allocations; thus resulting in significant cost savings. Using the information system view, there is no need to distinguish between cyber assets and critical cyber assets as all cyber assets within the information system are protected. Comments on Specific Requirements CIP 002 R3.1 NIST strongly recommends that a clear unambiguous definition of “routable protocol” be developed and, based on that definition, all routable protocols currently within the scope of the CIPs should be identified. All data encapsulated within a routable protocol should also be within the scope of the CIPs. CIP 002 R3.2 NIST recommends that “control center” should be replaced by “electronic security perimeter.” Nuclear Facility Exemption - In reference to section 4.2.1 of each CIP, NIST observes that the electric side of nuclear power plants can have an impact on the bulk electric sector. NIST suggests that the continuity of power aspects of nuclear facilities should be included in the scope of these standards. Therefore NIST recommends

Organization	Question 5:	Question 5 Comments:
		that the exemption statement: "Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission be changed to - Specific systems that are regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission (e.g., safety systems)." Wireless - NIST observes that the CIPs do not sufficiently address the security of wireless technologies, which include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. There appears to be an assumption in the CIPs that communication occurs solely over media. Consequently, NIST recommends that a clear, unambiguous definition of wireless technology be developed and security requirements for wireless technologies be included in the CIPs. Media Protection - NIST recommends that the CIPs? media protection requirements be expanded to cover all types of media. Because of the miniaturization and increased portability of digital media, protection of this media by a physical security perimeter is no longer adequate. Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). Information system media are also components of portable and mobile computing and communications devices (e.g., notebook computers, personal digital assistants, cellular telephones). The organization should have policy and procedures to protect and control information system media during transport outside the physical perimeter and restrict the activities associated with transport of such media to authorized personnel. For example, many organizations today prohibit removing laptop computers with unencrypted hard drives from the physical protection perimeter, and enforce this policy with unannounced inspection at the exits. Information system media is also a component of telephone systems that have the capability to store information (e.g., voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, policy should address the types of information stored on telephone voicemail systems that are accessible outside of physically protected areas.
Response: • Re Approach: "Critical Assets vs. Information Systems" – Control systems are specialized types of information systems. Accordingly, the SAR DT finds merit in this recommendation, particularly concerning data and control system operations centers. On the other hand, while substation and generation site networked-computing is growing more sophisticated, and at the same time general purpose information systems technology is being more widely employed. These operating environments are quite different than that of data and control system operations centers, and have a number of unique considerations. The SDT may consider splitting the CIP Standards requirements to address each of these two different operating environments. It may be appropriate to use "Information System" oriented thinking for data and control system operation centers, and "Critical Asset" oriented thinking for field and generation environs, at least until more mainstream networked "Information Systems" technology is		

Organization	Question 5:	Question 5 Comments:
more widely applied in those settings. The SAR DT does believe that a programmatic approach to control system cyber security is necessary. That is, control systems are just that – systems – and both control system components individually, and their working together in unison as an operational control system must be properly secured in a systematic manner. Per FERC Ruling 706, the SDT must consider adaptation of the NIST Security Risk Management Framework for electric sector control systems, and it would appear prudent to also consult similar bodies of work such as ISO/IEC 27001 and ISA99 as cross-checking resources to assure thorough and qualitative coverage of the issues. The SAR DT directs that this NIST recommendation be earnestly considered, regardless of whether or not the noted bifurcated approach described above is employed. • Re Comments on Specific Requirements: (1) Routable protocols: The SAR DT does not understand the intent and meaning of this comment. Use of "routable protocols" in original CIP drafting was intended in practical terms to refer to movement of data between and through subnetworks using IP datagrams employing a native addressing paradigm; this was specified as such generically due to the potential for other protocols with equivalent functionality to be used or emerge at a later date. Without further clarification from NIST, the SAR DT is unable to reply to this comment further, except to note that the entire discussion may be moot. Based upon the language of FERC Ruling 706, it may be at some point required that all control system critical cyber asset data communications must be secured regardless of protocol or media. Further clarification and discussion as to FERC's intent in its Directed Modifications will likely be necessary before the SDT can productively engage on this topic. (2) Re protection of encapsulated data: Relevant data or information must be appropriately protected regardless of state, i.e., in storage, being transmitted, or being processed. Communications transmission of critical cyber asset data/information must be protected regardless of media being employed, e.g., copper, glass, air. Also see the comment-reply below concerning media. (3) Re "Control Center": It is acknowledged that this term is a traditional colloquialism originating from the days when EMS/SCADA operator consoles and the control systems to which they were connected typically were geographically collocated. This obviously need not be the case today or in the future. The SDT will have to alternatively employ more appropriate terminology in the CIP update process. • Re Nuclear Facility Exemption: It is necessary to obtain further clarification as to the respective roles and responsibilities of Nuclear Plant Operators and Transmission Operators concerning the switchyard interface, and even potentially concerning assets within the nuclear plants themselves, e.g., non-safety systems components. Direct interaction between the SDT and NRC/CNSC ultimately may be needed to attain needed clarity as to respective scope of oversight responsibilities. A formal memorandum of understanding in some form also may be appropriate. The SDT will have to embrace the matter accordingly. • Re Wireless: The Standards do not preclude wireless as a medium and the SAR DT recommends the SDT provide any necessary clarification during the drafting phase. • Re Media Type: "NIST recommends that the CIPs media protection requirements be expanded to cover all types of media." The SAR DT agrees and directs attention to CIP-003, R4.1, which states: "The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type… "IAs NIST observes, there is a wide variety of media that can be employed, and each type should be evaluated for		

Organization	Question 5:	Question 5 Comments:
special considerations that may warrant explicit or additional treatment in the Standards' language. NIST's observation about voice mail systems is instructive as an example of the far ranging scope of considerations that have CIP significance, to wit, recordings of operator and/ or systems administrator interactions during a cyber security incident. Yet at the same time, it must be acknowledged that the media here is merely another instance of magnetic tape or disk storage. Finally, similar to the comment-reply under "wireless" above, detailed treatment of all manifestation of different storage media alternatives within the body of a Standard may not be appropriate, and might be better addressed in Supplemental Guidance or Guidelines. The SDT will have to weigh the alternative approaches in drafting. • In regard to participation on drafting phase, the SAR DT thanks you for your interest. The Standards Committee will solicit Standard Drafting team nominations and appoint them in accordance with segment representation and geographical diversity. Please look for the opening of nomination period on the NERC web pages. While not all nominations can be accommodated, interested persons are welcome and encouraged to remain engaged in the process. All drafting team meetings are open to all interested parties.		
We Energies	Yes	Compliance dates for any additional critical assets that need to be included as a result of the revised standards, or any new requirements for existing critical assets will require extended dates for compliance. The FERC 706 order will create changes in the NERC CIP requirements that will most likely be approved after some of the existing compliance dates have passed.
Response: We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance period for assets that are newly identified as critical, acquired through merger/acquisition or other means are included in a list of new stakeholder issues for the standard drafting team to address - these issues are in Attachment 3 of the revised SAR.		
NPCC	Yes	We do not want to limit the SAR to 706. We suggest that: 1) the inclusion/exclusion of Generation should be clarified 2) either delete CIP-001 or add it to CIP-008 3) add the definition of a control center 4) clarify that if a control center has a backup that demonstrates the control center's criticality, then the control center should be considered a Critical Asset
Response: Thank you for your input. 1. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available. 2. CIP-001 is not included in the scope of this project. The CIPC issued a recent guideline entitled, "Threat and Incident Reporting" wherein it aggregates reporting needs of NERC, DOE, ES-ISAC, DHS and RCMP. This guideline may found at www.esisac.com. 3. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. Definitions are included in that work scope especially when a word or phrase is used in specific sense and/or context. As a supplement to aid in		

Organization	Question 5:	Question 5 Comments:
		understanding the current CIP standards, the CIPC Risk Assessment Working Group (RAWG) is drafting guidance for use by the industry. A definition of control center is anticipated in that guidance. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available. 4. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the RAWG guidance, and is part of the clarity improvement work scope of the drafting team.
Southern Company Services, Inc.	Yes	For the future, implementation plan(s) should be reviewed to determine overlapping and interrelated issues of timing and revised appropriately (e.g. CIP-004, CIP-005 & CIP-006 may need to have requirements listed in better order so that background checks and training is done ?after? the electronic and physical perimeters are defined).Need flexibility to apply emerging technologies that improve the reliability of the bulk electric system rather than reducing reliability just to comply with the CIP standards. Need more granularities to the term ?critical?. There are indeed levels of criticality but these are not captured in the current standards. In much of the comments concerning NERC's CIP standards, one of the main objections raised is the great degree of flexibility in determining what assets are within scope. However from a utility viewpoint, the main issue with the NERC CIP standards is actually their inflexibility. With all the talk of choosing our own assets using "risk based methodologies", ?reasonable business judgment?, ?technical exceptions?, and ?acceptance of risk? it may be surprising to hear that anyone feels the standards are inflexible. However, the CIP-003 to CIP-009 standards are clearly written to apply to control room data centers and the types of cyber assets contained within them. These standards, which are appropriate for that environment, are then broadly applied to assets in the field such as substations and plants. The standards are inflexible in that they require this data-center like security around assets that are located in environments that are nothing like a data center. This base tension between data center environments and field environments is the reason that such flexibility must be included in CIP-002 and then sprinkled throughout the others. The issue with CIP-002 is actually in the inflexibility of CIP-003 to CIP-009. If the standard and its existing requirements were to be scoped to data-center environments for control systems, the standard would need much less flexibility throughout. A separate set of standards could then be developed through the NERC process that is more appropriate for assets located in the field. But with a scope of ?anything with a chip in it located anywhere in your service territory? then much flexibility is required. The CIP-002 standard only allows two classes of assets ? a cyber asset is either ?critical? and is to be protected to data-center level security or its ?not-critical? and is out of scope. The standard allows no middle ground, no ?risk based? protection, absolutely no flexibility in protecting those assets that fall somewhere in-between. It is purely binary. It is analogous to writing security standards appropriate for the cash processing operations of the central Federal Reserve banks that handle massive amounts of cash and then forcing them to apply to every location which houses any cash whatsoever, including all ATMs located in the field. The cost is prohibitive, you actually hinder the legitimate use of the asset, and the decrease in risk for the majority of the assets covered is negligible. For the most part, this tension revolves around the physical security and

Organization	Question 5:	Question 5 Comments:
		personnel aspects of the standard and their implementation for field locations. The standards go outside of typical technical, electronic access cyber security issues and enforce physical security and personnel-oriented security issues in a cyber asset focused vacuum. One cannot look at personnel or physical security issues holistically even on a site basis; no it must be focused solely on a particular cyber asset. This forces the industry to do costly things that bring little to no benefit or risk reduction and waste resources solely to be compliant to an inflexible standard that could be better spent reducing larger security vulnerabilities elsewhere. This is what causes most of the consternation and the desire to maintain great degrees of flexibility and control scopes within these standards.
Response: The SAR DT agrees with your suggestions to address additional implementation plans, consider the unique issues of implementing these standards to the substation and generating environment and to consider how to provide additional guidance in support of these standards. These have been included on a list of added stakeholder issues for the standard drafting team to address. These additional issues are in Attachment 3 of the revised SAR. With respect to defining additional gradation of critical assets, any added distinction made among critical assets may result in not protecting "lower level critical assets" in favor of the higher. It adds a level of complexity. In regard to emerging technologies, the standards do not preclude them nor prohibit their application. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available. While direction from FERC on the removal of "reasonable business judgment" and "acceptance of risk" will limit the amount of flexibility within the scope of the Standards, the drafting team must address these items mandated by FERC to be removed and the additional direction to narrowly define technical feasibility. Of the 8 standards that pertain to cyber security, including one which covers physical security of those cyber assets the "bar is set" by these standards. An entity may choose to exceed the standards. However at present there are no NERC reliability standards for the physical security of critical assets.		
Western Electricity Coordinating Council	Yes	WECC would like to see additional clarity around CIP-003-01.R3, specifically with respect to the difference between exception to policy and exception based on technical feasibility. Additionally, any potential situations other than technical feasibility which may commonly warrant exception should also be clarified within this effort. WECC agrees with FERC and the Blackout Report (FERC CIP NOPR, paragraph 139) that inappropriate disclosure of information should be prevented. This matter could be clarified by improving the language in CIP-

Organization	Question 5:	Question 5 Comments:
		003-01.R4 to describe the type of "protection" required. For example, language around digital protection such as encryption (at rest and in transit) for data elements and physical protections such as locked storage for maps, diagrams and other printed materials could be added. Additionally, verbiage describing if/how the information relevant to CIP-003-01.R4 is/isn't "data" that should be classified as a Critical Cyber Asset per the definition(s) provided in the NERC Glossary would be beneficial. Based on feedback from Registered Entities, there appears to be some confusion around how the requirements within CIP-005-01.R1.3 and CIP-006-01.R1.1 relate to one another. The crux of the issue is whether or not an entity can create one large Electronic Security Perimeter using Virtual Private Network (VPN) or similar technology to act as a "conduit" between physical facilities, or if they should maintain an individual Electronic Security Perimeter at each physical facility within a Physical Security Perimeter. WECC requests additions to the relevant CIP standards providing sufficient direction in this area.
Response: The SDT will address this issue as identified in Order 706 p.186 specifically the narrowing of the definition for "Technical Feasibility Exceptions". The SAR DT agrees with your suggestions to consider the issue of data versus information protection and to develop a guideline document to address extended LANs over multiple geographically dispersed locations. These suggestions have been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR..		
Ohio Valley Electric Corporation	Yes	How do the standards apply when a new Critical Cyber Asset is deployed? Is there a grace period to bring it into compliance? The drafting team should address this issue.
Response: We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR..		
Midwest ISO	Yes	How do the standards apply when a new Critical Cyber Asset is deployed? Is there a grace period to bring it into compliance? The drafting team should address this issue.
Response: We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR..		
LK4 Technology Corporation	Yes	Proof of policy relating to risk assessment produces "Auditable Compliance". This was the standard adopted decades ago by the National Security Agency and then NIST.
Response: Thank you for your comment and input.		
WECC-NERC PMO - PacifiCorp	Yes	The order as written does not adequately address the common security practice of using site-to-site VPN technologies to extend a trusted security zone across multiple locations. With respect to the CIPRS, where the

Organization	Question 5:	Question 5 Comments:
		VPN endpoints are under the sole control of and within the Physical Security Perimeters of the same responsible entity, a properly configured VPN should be considered adequate mitigation of physical attacks against the communications link.
Response: The SAR DT recommends that the SDT consider developing a guideline document to address extended LANs over multiple geographically dispersed locations. This has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR.		
Hydro One Networks Inc.	Yes	There is now an opportunity to extend the SAR's scope beyond the content in the FERC Order, provided that FERC timelines can still be met. Interpretations which were made subsequent to the standards should be formally codified into the appropriate places in the standards, such as the CIP-006 interpretation. Similarly, experience from entities implementing the Cyber Standards should be taken into consideration as there have been valuable lessons learned.
Response: Thank you for your input. These additional stakeholder issues are included in Attachment 3 of the revised SAR. Revisions will incorporate the clarifications from the Interpretation of CIP-006-1 Requirement 1.1.		
FirstEnergy Corp.	Yes	Although the Order discusses contractors and vendors, the standards may need more clarity with regard to how far a responsible entity must go to assure matters such as background checks are properly completed. The team should consider adding to the Scope of the SAR: "With regard to third-party vendors and contractors, provide clarification and additional guidance as to how much a responsible entity may rely on the processes and procedures of contractors and vendors that support the critical infrastructure of that responsible entity under the CIP standards and still be compliant with the standard."
Response: The SAR DT has added your suggestion to Attachment 3 of the revised SAR.		
WECC (Steve Rueckert)	Yes	SAR should include an item that CIP2-9 explictly addresses serial devices as the industry seems to be challenged in situations where there are hybrid devices that use both serial and routable protocols. An example is where a Critical Cyber Asset is a serial device connected directly to a router, thus converting it to a routable protocol. This is not a recommendation that the CIP2-9 scope be expanded to include serial devices, but that CIP2-9 provide explicit guidance.
Response: The SAR DT thanks the commenter for the input. Your suggestion to consider modifying the standard to clarify the issue with respect to hybrid devices that use both serial and routable has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR.		
Southwest Power Pool	Yes	Comments: The four tables in the Implementation Plan prescribe the initial compliance schedule for a registered entity, with Table 4 addressing new entities that register in the future. But there is no table prescribing a schedule in which an existing registered entity can bring a newly identified critical asset and its critical cyber assets into compliance. While not expected to change frequently, the critical asset list can change for any number of valid reasons (including new guidance from FERC, NERC or the Regional Entities as to what constitutes a "critical asset" for purposes of the CIP Standards), and the registered entity needs to have an appropriate period of time

Organization	Question 5:	Question 5 Comments:
		in which to achieve compliance with the standards for that asset. In the absence of a compliance schedule, no guidance is available to either the registered entity or the auditor. A new table should be developed defining a compliance schedule for standards CIP-003 through CIP-009 applicable to newly identified critical assets and based upon the date of the risk assessment. The new table should give due consideration to those CIP requirements that are broadly applicable to the entity and should already be in compliance, and those requirements that require new resources and effort and should be afforded adequate time to reach compliance. That consideration should include consideration whether or not the entity had previously identified any critical assets.
Response: We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR.		
Duke Energy	No	However the House Subcommittee concerns about critical infrastructure protection are not addressed. After implementing FERC's direction the CIP standards will still only cover a small fraction of the assets identified by the House Subcommittee. Because of this, the CIP standards will continue to come under criticism.
Response: Thank you for your comment and input. The NERC Reliability Standards are focused upon ensuring reliable operation of the BES as a whole, not the continued operation of an individual asset.		
AEP	No	
Dominion Resources Services, Inc.	No	
ElectriCities of North Carolina, Inc.	No	
Public Service Commission of South Carolina	No	
Oncor Electric Delivery Company LLC	No	
Ontario IESO	No	
Electric Power	No	

Organization	Question 5:	Question 5 Comments:
Supply Association		
M-S-R Public Power Agency	No	
American Electric Power	No	
PJM Interconection	No	
Detroit Edison	No	
Ontario Power Generation	No	
Coral Power, L.L.C.		no comment
United Illuminating	No	

6. If you have any other comments on this SAR that you haven't already provided in response to the prior five questions, please provide them here.

Summary Consideration: There are several comments encouraging the SDT work with the regional entities and the FERC which are acknowledged and appreciated. The SAR DT disagreed with a commenter's recommendation that Transmission Service Providers not be subject to these CIP Standards. The SAR DT believes that the functions performed by the TSP are essential to real time reliable operation of the BES and therefore should be subject to the CIP Standards. The existing CIP-002-1 through CIP-009-1 already apply to the Transmission Service Provider.

The SAR DT concurs with a commenter with respect to focusing the SDT upon the NIST framework and also agrees that other relevant publications/technical reports such as from the MITRE corporation, the DHS and National Laboratories should also be considered. These have been added to the SAR.

Organization	Question 6 Comments:
XcelEnergy	It is not clear that the current body of CIP standards was based on any real assessment or understanding of potential risks to the bulk electric system of terroristic threats. Rather, it appears that the standards were developed at the micro level based on perceived risks to specific pieces of equipment without a holistic understanding of how grid systems work or where the greatest vulnerabilities really lie. We believe that the next round of CIP standards should be guided by a more clearly defined set of risks which can result in a more focused and effective set of compliance expectations.
Response: Thank you for your comment and input. The NERC Reliability Standards are focused upon ensuring reliable operation of the BES from a broad spectrum of threats. The SAR DT has added your suggestion to a list of issues for the standard drafting team to address in Attachment 3 of the revised SAR.	
PJM Interconection	It is vitally important that NERC and the Regional Entities work together to provide a common set of audtiting guidelines so that they may be distributed to the industry to help with compliance efforts. Each Responsible Entity has been left with the task of interpreting the CIP Standard requirements and have no way of telling whether their efforts and opinions are correct. There is a very real and serious concern by the Responsible Entities that they could be found in non-compliance due to a difference in opinion or interpretation of any given CIP Standard requirement. With an aggressive Implementation Schedule, these concerns should be addressed as soon as possible. After the SAR process is completed, the same guidance will need to be developed and produced to the Responsible Entities in the industry.
Response: The Compliance Program is currently developing Reliability Standard Audit Worksheets (RSAWs) for the existing CIP Standards. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the CIPC Risk Assessment Working Group (RAWG) guidance, and is also part of the drafting team work scope. Improving clarity of the standard requirements is among the standard drafting team's tasks.	

Organization	Question 6 Comments:
Pacific Gas and Electric Company	1) Suggest that FERC be an active participant in drafting both the CIP 2-9 SAR and subsequent standards revisions 2) Emphasize the need for the scope of the revisions to CIP002 to address the need for a consistent framework to identify critical assets.
Response: 1. The standard development process encourages FERC participation in clarifying the directives in Order 706. 2. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the CIPC Risk Assessment Working Group (RAWG) guidance, and is part of the clarity improvement work scope of the drafting team.	
Transmission Agency of Northern California	The Transmission Agency of Northern California (?TANC?) appreciates the opportunity to comment on this SAR. TANC believes that the applicability of the Cyber Security Standards (i.e. CIP-002-1 through CIP-009-1) to Transmission Service Providers (?TSP?) is inappropriate and unnecessarily burdensome on entities registered as TSP, and thereby requests that this applicability be removed in the revised standards. FERC Order 706 conditionally approved the current versions of the Cyber Security Standards and directed modifications to the standards that are initiated by this SAR. In Order 706 at Paragraph 49, FERC cautions against an "overly-expansive" approach "requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry. "TANC contends that business practices related to the TSP function do not involve any Critical Cyber Assets and therefore concludes that the current TSP applicability of the revised standards is inappropriate. In its "Glossary of Terms Used in Reliability Standards" as adopted by the NERC Board of Trustees on February 12, 2008, NERC provides the following definitions of terms essential to the applicability of the CIP standards: Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data. Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets. The TSP's primary functions are administering the transmission tariff and processing transmission service requests in accordance with its tariff and transmission service agreements. In this capacity, the TSP calculates Available Transfer Capability, approves transmission service requests from customers, and validates e-tags received from the Interchange Authority for confirmation that the interchange schedule references a valid transmission reservation. Computer systems used by the TSP are limited to the OASIS and e-tagging systems, both of which are typically third-party hosted web-based applications. Many TSPs use a common third-party vendor for these systems. As these systems are typically hosted externally to the TSP, there are no Critical Cyber Assets necessarily owned by the TSP, and applying the CIP standards individually to TSPs imposes unnecessary costs of compliance on these entities. It is also unlikely that degradation of these systems used by the TSP would affect the reliability or operability of the Bulk Electric System because these systems are not involved in actual Bulk Electric System operations. The NERC Functional Model (Version 3) states that the Transmission Service Provider does not itself have a role in maintaining system reliability in real time ? that is the

Organization	Question 6 Comments:
	Reliability Coordinator's and Transmission Operator's responsibility. The TSP's systems support commercial activities involved in the administration of the transmission tariff and forward planning activities (information related to facility ratings and transfer capabilities) that do not pose the same degree of risk to reliability as systems involved in transmission system operations, monitoring and controls. Continuing to include TSP in the applicability section of the revised standards causes every entity registered as TSP to comply with the requirements of CIP-002 only to annually confirm that they have no Critical Cyber Assets related to that function. Such an exercise would be unnecessarily burdensome to entities that are already incurring high costs to comply with the appropriately applicable standards.
Response: The SAR DT thanks the commenter for its input. The team does not agree with the argument of the commenter to remove TSP from applicability of the CIP standards. The Functional Model identifies the following tasks performed by a TSP: • TSPs approves or denies transmission service requests from PSEs, GOPs and LSEs. • Confirms transmission service requests to IAs • Provides loss allocation to BAs The SAR DT believes that these functions are essential to real time reliable operation of the BES and therefore should be subject to the CIP Standards. Note that the existing approved CIP-002-1 through CIP-009-1 all list the Transmission Service Provider as a responsible entity. As the standards are refined, there is an opportunity to look more closely at each of the requirements and, where applicable, to provide greater clarity in identifying the responsible entity. Refer to CIP-002 for criteria to determine critical asset identification.	
NPCC	Of concern is the one size fits all approach by the standards, in that many requirements attempt to address themselves equally to several different cyber environments. NPCC sees major differences with respect to control center environments and configurations, which are more like typical IT Enterprise style environments utilizing readily available hardware, software, and application platforms and processes. Generators, substations, and other small or remote facilities, have older legacy and single function system and process configurations, which can be best described as atypical to control room configurations. The problem lies in the difficulty of trying to define technical requirements that can effectively address the different kinds of cyber environments. The result too often is a requirement that serves no one environment well. The standards attempt to resolve this by leaving it to the Entity to try and figure out what the real requirement is for them, and wondering whether their implementation will be compliant. Therefore NPCC believes that such requirements need to specify which cyber environments they apply to, and ensure they provide appropriate clarity and direction to that environment.
Response: The SAR DT acknowledges that the substation environment is gradually becoming comparable in terms of cyber security importance with control center environments. The following issues have been added to Appendix 3 of the revised SAR: 1. Consider the unique issues of implementing these standards to the substation and generating environment sub station considerations is among these issues.	

Organization	Question 6 Comments:
2. Consider how to provide additional guidance on control centers in support of these standards.	
Southern Company Services, Inc.	We'd ask NERC to consider informing the industry early and often as to the various drafting options you would consider on these CIP standards.
Response: The Standard Development Procedure describes the process in detail. It can be found on the NERC website at the following URL: http://www.nerc.com/standards/newstandardsprocess.html Meetings of the SDT and conference calls are open to interested observers with prior notice.	
Western Electricity Coordinating Council	WECC recognizes and supports the shift toward standards that more closely align with the NIST SP800 series. Opportunities during this revision effort should be taken to move the existing CIP standards in that direction. Inclusion of appropriate elements from various Special Publications, and not just SP800-53x, should be considered since there is overlap and interplay between the various SP800 documents. WECC acknowledges the importance of protecting Critical Cyber Assets; however, at some point in time if not part of this revision process, physical security of the Critical Assets must be addressed.
Response: There are several documents that have relevance to Cyber Security that have been circulating in industry. A MITRE corporation technical report (MTR070050) analyzes current NERC standards in comparison to NIST SP-800 standard. The MITRE report recommends, "NIST and FERC should work together to develop an interpretation of SP 800-53 that is applicable to both public and private entities in the electric power sector. Another MITRE corporation report offers various approaches to control system security. The National Institute of Standards and Technology has offered its NIST SP 800-53 standard, "Recommended Security Controls for Federal Information Systems" for NERC drafting team consideration and adoption. There is also a Department of Homeland Security report, "Catalog of Control Systems Security: Recommendations for Standards Developers - January 2008" detailing recommendations to increase the security of control systems from both physical and cyber attacks. The SAR DT has explicitly included the Order 706 recommendation to consider features of the NIST framework and other relevant publications/technical reports such as from the MITRE corporation, the DHS and National Laboratories in the revision of the CIP Standards. There are currently no standards for physical security of critical assets however a SAR may be initiated by any stakeholder for the Standards Committee to consider.	
Duke Energy	It appeared that the original drafting team had a strong focus on Energy Management systems supporting Control Centers. When the same CIP standards were applied to Substations, some of the requirements, i.e., patch management, anti virus, etc., had limited applicability. Additional specific expertise is needed on the drafting team to ensure the standards are equally applicable to all relevant Critical Assets. Any changes (particularly in the identification of Critical Assets) MUST include corresponding changes to the implementation plan.

Organization	Question 6 Comments:
Response: Thank you for your input. Diverse subject matter experts are included on this SAR DT and will be sought for participation on the SDT. Note that the nomination form used to solicit volunteers for this SAR DT specifically mentioned that the Standards Committee was seeking volunteers who have, "Experience developing or implementing cyber security policies and procedures; experience implementing or managing the implementation of the cyber security standards is preferred."	
Ontario IESO	The four tables in the Implementation Plan prescribe the initial compliance schedule for a registered entity, with Table 4 addressing new entities that register in the future. But there is no table prescribing a schedule in which an existing registered entity can bring a newly identified critical asset and its critical cyber assets into compliance. While not expected to change frequently, the critical asset list can change for any number of valid reasons, and the registered entity needs to have an appropriate period of time in which to achieve compliance with the standards for that asset. In the absence of a compliance schedule, no guidance is available to either the registered entity or the auditor. A new table should be developed defining a compliance schedule for standards CIP-003 through CIP-009 applicable to newly identified critical assets and based upon the date of the risk assessment. The new table should give due consideration to those CIP requirements that are broadly applicable to the entity and should already be in compliance, and those requirements that require new resources and effort and should be afforded adequate time to reach compliance. That consideration should include consideration whether or not the entity had previously identified any critical assets. The applicability of the standards should be expanded to include LSEs, which own BES transmission and/or distribution facilities.
Response: We agree and thank you for your input. Note that every standard drafting team is required to post, as part of its work scope, an implementation plan. The SAR DT has added your suggestion of addressing the time needed to become compliant with the standards when an entity has assets that are newly identified as critical, acquired through merger/acquisition or other means, to a list of items for the drafting team to address in Attachment 3 of the revised SAR.	
FirstEnergy Corp.	FE provides the following additional comments: 1. The Scope will understandably address the FERC directed changes from Order 706. However, there may be instances in the Order where FERC believes a comment is valid but did not specifically direct a change but may merit a further look by the CIP drafting team. Also, as the drafting team work is underway, issues may arise and become more evident in the realm of critical infrastructure protection that may show a glaring need for new requirements. We want to assure that the SAR is not overly narrow in scope as to prevent the drafting team from proposing additional requirements that are both needed and sound. 2. Implementation - Throughout this development, the team should keep in mind that there is much work underway and completed by responsible entities in preparation for compliance with these standards as written today. Once changes are made, these entities should be given a reasonable amount of time to make any

Organization	Question 6 Comments:
	necessary adjustments. Furthermore, any new implementation schedule should start after the current implementation schedule is complete. 3. The SAR proposes to address the following NERC "principles": Reliability Principle 4 [Plans for emergency operation and system restoration of interconnected bulk electric systems shall be developed, coordinated, maintained and implemented] and Market Interface Principle 4 [An Organization Standard shall not preclude market solutions to achieving compliance with that standard]. It is not clear why the SAR should specifically address these principles. Are these not general principles applicable to every standard? If not, then why not address the other 6 Reliability principles and other 4 Market Interface principles? 4. NERC approved interpretation of CIP-006-1 R1.1, as well as ongoing interpretation development of CIP-006-1 R1.2 and CIP-005-1 Requirement 1 (per NERC project 2007-30) should be incorporated into the scope of the development of these standards. Also, in the SAR under "Industry Need", reference should be made to "CIP-006-1a" which has incorporated the NERC approved interpretation of R1.1 in Appendix 1.
Response: 1. The SAR DT asserts that all matters identified in the Order 706 will be addressed. The SAR will define the scope per the Standard Development Procedure. 2. The SDT will be making the determinations for appropriate implementation plan in its drafting work. 3. Each standard supports at least one reliability principle and complies with all market interface principles. 4. As a matter of course, any approved interpretation in force at the time of standard revision work will be incorporated into the revised version.	
WECC (Steve Rueckert)	1) Suggest that FERC be an active participant in drafting both the CIP 2-9 SAR and subsequent standards revisions if permissible2) Emphasize the need for the scope of the revisions to CIP002 to address the need for a consistent framework to identify critical assets.
Response: 1. The standard development process encourages FERC participation in clarifying its directives. 2. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the CIPC Risk Assessment Working Group (RAWG) guidance, and is part of the clarity improvement work scope of the drafting team.	
Southwest Power Pool	There is concern that entities have internal security measures in place that may exceed the CIP requirements. The SAR should include in its scope that the standard clarify measures for compliance will be relegated to the FERC approved requirements and not any internal policies.
Response: The SAR DT thanks you for your comment. The SAR DT has added a list of stakeholder issues for the standard drafting team to	

Organization	Question 6 Comments:
address – and the issue where an organization has implemented an information security policy and program that includes requirements beyond the NERC CIP requirements is among those issues. The issue will include review of FERC Order 706 paragraph 377 and the pertinent requirements and compliance information of CIP-003 to make it clear that only non-compliance with the NERC CIP requirements will be subject to non-compliance findings. These additional issues are included in Attachment 3 of the revised SAR.	
Coral Power, L.L.C.	None
Electric Power Supply Association	no additional comments
M-S-R Public Power Agency	None.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009)
Request Date March 1, 2008 Revision Date June 9, 2008
Approved by Standards Committee for standard development on July 10, 2008

SAR Requester Information		**SAR Type** (*Check a box for each one that applies.*)	
Name	Dave Norton	☐	New Standard
Company	Entergy	☒	Revision to existing Standards
Telephone Fax	(504) 576-5469	☐	Withdrawal of existing Standard
E-mail	dnorto1@entergy.com	☐	Urgent Action

Purpose (Describe what the standard action will achieve in support of bulk power system reliability.)

To protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

Implement Changes to the following Cyber Security Standards as indicated in FERC Order 706:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Brief Description (Provide a paragraph that describes the scope of this standard action.)

This set of revisions in this project includes:

- Modifying the standards so they conform to the latest approved versions of the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1.
- Addressing the directives issued by FERC, in Order 706 relative to the approved Cyber Security Standards CIP-002-1 through CIP-009-1. Refer to http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf for the complete text of the final order. Specific requirements from the Order are identified in Attachment 2.
    - Emphasis on Order 706 directive for NERC to address revisions to the CIP standards considering applicable feature of the NIST Security Risk Management Framework among other resources.
- Incorporating clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

Additional issues identified by stakeholders during the posting of this SAR are listed in Attachment 3.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.)

This project requires reviewing each of the standards to ensure that it conforms to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure as outlined in the Standard Review Guidelines (Attachment 1).

This proposed standards drafting project includes addressing all of the directed modifications identified in the FERC Final Order 706. These directives are summarized in Attachment 2.

Revisions will incorporate the clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

Revisions should consider other Cyber-related standards, guidelines and activities:

- Consider adopting the NIST Security Risk Management Framework (includes GAO, OMB and FIPS)
- Consider other cyber security related documents such as NIST, ISO 27000 Family, CIPC WG Risk Assessment Guideline, MITRE corporation technical report, DHS, National Laboratories papers, DOE 417, IEC, ISA, etc.
- Stay apprised of coordination work between FERC, NEI and NRC in regard to the nuclear facility exemption issue with respect to regulatory gaps. As necessary modify the standards to reflect current determinations.

Revisions should consider the additional issues identified by stakeholders in Attachment 3.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Regional Entity	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☒	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Related Standards

Standard No.	Explanation
CIP-001	Sabotage Reporting (no change proposed)
CIP-002	Critical Cyber Asset Identification – FERC directed modifications
CIP-003	Security Management Controls – FERC directed modifications
CIP-004	Personnel and Training – FERC directed modifications
CIP-005	Electronic Security Perimeter – FERC directed modifications
CIP-006	Physical Security – FERC directed modifications
CIP-007	Systems Security Management – FERC directed modifications
CIP-008	Incident Reporting and Response Planning – FERC directed modifications
CIP-009	Recovery Plans – FERC directed modifications

Related SARs

SAR ID	Explanation
None	

Regional Variances

Region	Explanation
ERCOT	None
FRCC	None
MRO	None
NPCC	None
SERC	None
RFC	None
SPP	None
WECC	None

Attachment 1 - Standard Review Guidelines

Technical Basis in Engineering and Operations
Is this reliability standard based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field?

Purpose
Does this reliability standard have a clear statement of purpose that describes how the standard contributes to the reliability of the bulk power system? Each purpose statement should include a value statement.

Applicability
Does this reliability standard clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted? Where multiple functional classes are identified is there a clear line of responsibility for each requirement identifying the functional class and entity to be held accountable for compliance? Does the requirement allow overlapping responsibilities between Registered Entities possibly creating confusion for who is ultimately accountable for compliance?

Does this reliability standard identify the geographic applicability of the standard, such as the entire North American bulk power system, an interconnection, or within a regional entity area? If no geographic limitations are identified, the default is that the standard applies throughout North America.

Does this reliability standard identify any limitations on the applicability of the standard based on electric facility characteristics, such as generators with a nameplate rating of 20 MW or greater, or transmission facilities energized at 200 kV or greater or some other criteria? If no functional entity limitations are identified, the default is that the standard applies to all identified functional entities.

If the applicability is to a set of responsible entities that have criteria other than the criteria used in the compliance registration process, then the applicability section of the standard should include the reliability-related reason for the unique applicability criteria.

Effective Dates
Must be 1st day of 1st quarter after entities are expected to be compliant – must include time to file with regulatory authorities and provide notice to responsible entities of the obligation to comply. If the standard is to be actively monitored, time for the Compliance Monitoring and Enforcement Program to develop reporting instructions and modify the Compliance Data Management System(s) both at NERC and Regional Entities must be provided in the implementation plan. The effective date should be linked to the applicable regulatory approvals – here is the default sentence to use for standards that should become effective as soon as possible:

First day of first calendar quarter after applicable regulatory approval (or, in those jurisdictions where regulatory approval is not required, the standard becomes effective on the first day of the first calendar quarter after BOT adoption.)

Performance Requirements
Does this reliability standard state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest?

Does each requirement identify who shall do what under what conditions and to what outcome?

Fill-in-the-blank Requirements
Do not include any 'fill-in-the-blank' requirements. These are requirements that assign one entity responsibility for developing some performance measures without requiring that the performance measures be included in the body of a standard – then require another entity to comply with those requirements.

Every reliability objective can be met, at least at a threshold level, by a North American standard. If we need regions to develop regional standards, such as in under-frequency load shedding, we can always write a uniform North American standard for the applicable functional entities as a means of encouraging development of the regional standards.

Requirements for Regional Reliability Organization
Do not write any requirements for the Regional Reliability Organization. Any requirements currently assigned to the RRO should be re-assigned to the applicable functional entity. If the requirement can only be performed at a regional level, assign the requirement to the Regional Entity, not the RRO.

Violation Risk Factors
Each requirement must have an associated Violation Risk Factor (VRF). Avoid assigning a VRF to sub-requirements. If a sub-requirement needs a VRF that is different from the VRF assigned to the main requirement, then consider sub-dividing the requirement into multiple requirements. The VRF identifies the reliability-related risk of violating a requirement.

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures;

or a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures;

or a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system.

A requirement that is administrative in nature and is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk

electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

Time Horizon
The drafting team should also indicate the time horizon available for mitigating a violation to the requirement using the following definitions:

- **Long-term Planning** — a planning horizon of one year or longer.
- **Operations Planning** — operating and resource plans from day-ahead up to and including seasonal.
- **Same-day Operations** — routine actions required within the timeframe of a day, but not real-time.
- **Real-time Operations** — actions required within one hour or less to preserve the reliability of the bulk electric system.
- **Operations Assessment** — follow-up evaluations and reporting of real time operations.

Measurability
Is each performance requirement stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement?

Does each performance requirement have one or more associated measures used to objectively evaluate compliance with the requirement? Measures should comply with the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" reference document.

If performance results can be practically measured quantitatively, are metrics provided within the requirement to indicate satisfactory performance?

Violation Severity Levels
The drafting team should indicate a set of violation severity levels that can be applied for the requirements within a standard. ('Violation severity levels' replace existing 'levels of non-compliance.') The violation severity levels must be applied for each requirement and may be combined to cover multiple requirements, as long as it is clear which requirements are included and that all requirements are included.

The violation severity levels should be based on the following definitions and the latest version of the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards":

- **Lower: mostly compliant with minor exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more minor details.
- **Moderate: mostly compliant with significant exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more significant elements.
- **High: marginal performance or results** — The responsible entity has only partially achieved the reliability objective of the requirement and is missing one or more significant elements.
- **Severe: poor performance or results** — The responsible entity has failed to meet the reliability objective of the requirement.

Compliance Enforcement Authority
Replace, 'Regional Reliability Organization' with 'Regional Entity'

Replace, 'NERC' with 'ERO'
In situations where the Regional Entity is the responsible entity, or where a responsible entity works for the Regional Entity, the Compliance Enforcement Authority is the ERO. In all other situations, the Regional Entity is the Compliance Enforcement Authority.

Compliance Monitoring Period and Reset Timeframe
In all cases, enter, 'Not applicable.' (These terms are associated with an older version of the sanctions table. The next time the Reliability Standards Development Procedure is updated, the procedure will be revised to omit references to 'compliance monitoring period' and 'reset timeframe'.)

Data Retention
Use the data retention periods proposed in the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" document unless there is a justifiable reason for proposing other data retention periods.

Compliance Monitoring Processes
The list of compliance monitoring processes used with each standard should comply with the proposed list of processes identified in the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" reference document. In the standard, list the compliance monitoring processes under 'Additional Compliance Information.'

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Periodic Data Submittals
- Exception Reporting
- Complaints

Associated Documents
We will delay populating this section of the standard with a list of 'related' standards because standards are all being changed and many will have new numbers. We should limit the references to those support documents that are useful in complying with the standard.

Functional Model Version 3
Review the requirements against the latest descriptions of the responsibilities and tasks assigned to functional entities as provided in pages 13 through 53 of the draft Functional Model Version 3.

Completeness
Is this reliability standard complete and self-contained? Does the standard depend on external information to determine the required level of performance?

Clear Language
Is the reliability standard stated using clear and unambiguous language? Can responsible entities, using reasonable judgment and in keeping with good utility practices, arrive at a consistent interpretation of the required performance?

Consistent Terminology
To the extent possible, does this reliability standard use a set of standard terms and definitions that are approved through the NERC reliability standards development process?

If the standard uses terms that are included in the NERC Glossary of Terms Used in Reliability Standards, then the term must be capitalized when it is used in the standard. New terms should not be added unless

they have a ‘unique’ definition when used in a NERC reliability standard. Common terms that could be found in a college dictionary should not be defined and added to the NERC Glossary.

Practicality
Does this reliability standard establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter?

Consequences for Noncompliance
In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, are the consequences of violating a standard clearly known to the responsible entities?

Attachment 2 (this is a large attachment and is in a self-contained file)

Attachment 3

Stakeholder Issues and Recommendations Identified During Initial SAR Posting

Industry Education

- Consider what to do with the existing FAQ document e.g., modify, replace.
- Consider how to provide additional guidance in support of these standards, e.g., Technical Reference documents, guidelines, white papers.
- Consider development of a guideline document to address extended LANs over multiple geographically dispersed locations.

Balloting and Implementation

- Determine the timing and grouping of revisions to be submitted to industry for comment and ballot, e.g., multi-phase or other approach.
- Determine the optimum implementation plan for revised CIP standards in this project.
- Address when newly identified critical assets or critical cyber assets, newly acquired equipment or assets, etc. must come into compliance with CIP standards.
- Address compliance issue where internal requirements exceed NERC requirements. Clarify in view of language contained in FERC Order 706 paragraph 377.

Clarify Existing Requirements

- Consider the need for different requirements for different environments e.g., control center, substation and generation plant.
- Clarify how serial and wireless devices are subject to these standards. Refer to pp 278 and 285 of FERC Order 706.

Other Issues

- Consider issues surrounding protection of data in motion.
- Consider the issue of hybrid devices that use both serial and routable protocols.
- Consider the issue of data versus information (electronic and/or hardcopy lists, drawings, etc.) protection including transport and transmittal of such information.
- Consider a clearly defined set of risks which can result in a more focused and effective set of compliance expectations.
- With regard to third-party vendors and contractors, provide clarification and additional guidance as to how much a responsible entity may rely on the processes and procedures of contractors and vendors that support the critical infrastructure of that responsible entity under the CIP standards and still be compliant with the standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009)
Request Date March 1, 2008 Revision Date June 9, 2008
Approved by Standards Committee for standard development on July 10, 2008

SAR Requester Information	**SAR Type** (*Check a box for each one that applies.*)	
~~Name NERC Staff~~Name Dave Norton	☐	New Standard
~~Primary Contact Scott R. Mix~~Company Entergy	☒	Revision to existing Standards
Telephone ~~215-853-8204~~(504) 576-5469 Fax	☐	Withdrawal of existing Standard
~~E-mail scott.mix@nerc.net~~E-mail dnorto1@entergy.com	☐	Urgent Action

Purpose (Describe what the standard action will achieve in support of bulk power system reliability.)

To protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

Implement Changes to the following Cyber Security Standards as indicated in FERC Order 706:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Brief Description (Provide a paragraph that describes the scope of this standard action.)

This set of revisions ~~will implement the modifications directed~~in this project includes:

- Modifying the standards so they conform to the latest approved versions of the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1.
- Addressing the directives issued by FERC, in ~~**their**~~ Order 706~~,~~ relative to the approved Cyber Security Standards CIP-002-1 through CIP-009-1. Refer to http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf for the complete text of the final order. Specific requirements from the Order ~~**will be**~~are identified ~~**during the SAR and/or Standards Drafting process.**~~ in Attachment 2.
    - ~~**In addition, the drafting team will modify the standards so they conform to the latest approved versions of the Reliability Standards Development Procedure and the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1.**~~Emphasis on Order 706 directive for NERC to address revisions to the CIP standards considering applicable feature of the NIST Security Risk Management Framework among other resources.
- Incorporating clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

~~NOTE:~~ Additional issues identified by stakeholders during the posting of this SAR are listed in ~~a supplementary SAR. The supplementary SAR will be posted for industry comment, and if supported by stakeholders, will be appended to this SAR~~Attachment 3.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.)

This project requires reviewing each of the standards to ensure that it conforms to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure as outlined in the Standard Review Guidelines (Attachment 1).

This proposed standards drafting project ~~will address~~includes addressing all of the directed modifications identified in the FERC Final Order 706. ~~There are a significant number of directed modifications to the set of cyber security standards. Some of them are of low consequence, and low controversy, while others are more significant changes, with more contentious issues. There may be a third set of changes that are in between these two extremes. Whether there are two or three "classes" of changes will be left to the Standards Drafting Team.~~These directives are summarized in Attachment 2.

~~As envisioned, the standard drafting team will address the "low hanging fruit" and rapid turn-around issues first, working on some of the more contentious issues while the less contentious issues are in either comment or ballot mode. This may allow for multiple revisions to the standards where some changes are reviewed by industry, balloted, and submitted for approval during the development and comment cycle of the remaining contentious issues.~~ Revisions will incorporate the clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

~~The end result of this SAR may be more than one set of revised standards submitted for approval.~~Revisions should consider other Cyber-related standards, guidelines and activities:

~~This SAR also proposes to add the following from the original Cyber Security Standards SAR finalized on March 8, 2004:~~

~~Regional Entities and Purchasing-Selling Entity functions to the applicability section of the standards.~~

~~Reliability and Market Interface Principle 4 (plans for emergency operation and system restoration).~~

~~If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator – see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR.~~

- Consider adopting the NIST Security Risk Management Framework (includes GAO, OMB and FIPS)
- Consider other cyber security related documents such as NIST, ISO 27000 Family, CIPC WG Risk Assessment Guideline, MITRE corporation technical report, DHS, National Laboratories papers, DOE 417, IEC, ISA, etc.
- Stay apprised of coordination work between FERC, NEI and NRC in regard to the nuclear facility exemption issue with respect to regulatory gaps. As necessary modify the standards to reflect current determinations.

Revisions should consider the additional issues identified by stakeholders in Attachment 3.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Regional Entity	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☒	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Related Standards

Standard No.	Explanation
CIP-001	Sabotage Reporting (no change proposed)
CIP-002	Critical Cyber Asset Identification – FERC directed modifications
CIP-003	Security Management Controls – FERC directed modifications
CIP-004	Personnel and Training – FERC directed modifications
CIP-005	Electronic Security Perimeter – FERC directed modifications
CIP-006	Physical Security – FERC directed modifications
CIP-007	Systems Security Management – FERC directed modifications
CIP-008	Incident Reporting and Response Planning – FERC directed modifications
CIP-009	Recovery Plans – FERC directed modifications

Related SARs

SAR ID	Explanation
None	

Regional Variances

Region	Explanation
ERCOT	None
FRCC	None
MRO	None
NPCC	None
SERC	None
RFC	None
SPP	None
WECC	None

Attachment 1 - Standard Review Guidelines

Technical Basis in Engineering and Operations
Is this reliability standard based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field?

Purpose
Does this reliability standard have a clear statement of purpose that describes how the standard contributes to the reliability of the bulk power system? Each purpose statement should include a value statement.

Applicability
Does this reliability standard clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted? Where multiple functional classes are identified is there a clear line of responsibility for each requirement identifying the functional class and entity to be held accountable for compliance? Does the requirement allow overlapping responsibilities between Registered Entities possibly creating confusion for who is ultimately accountable for compliance?

Does this reliability standard identify the geographic applicability of the standard, such as the entire North American bulk power system, an interconnection, or within a regional entity area? If no geographic limitations are identified, the default is that the standard applies throughout North America.

Does this reliability standard identify any limitations on the applicability of the standard based on electric facility characteristics, such as generators with a nameplate rating of 20 MW or greater, or transmission facilities energized at 200 kV or greater or some other criteria? If no functional entity limitations are identified, the default is that the standard applies to all identified functional entities.

If the applicability is to a set of responsible entities that have criteria other than the criteria used in the compliance registration process, then the applicability section of the standard should include the reliability-related reason for the unique applicability criteria.

Effective Dates
Must be 1st day of 1st quarter after entities are expected to be compliant – must include time to file with regulatory authorities and provide notice to responsible entities of the obligation to comply. If the standard is to be actively monitored, time for the Compliance Monitoring and Enforcement Program to develop reporting instructions and modify the Compliance Data Management System(s) both at NERC and Regional Entities must be provided in the implementation plan. The effective date should be linked to the applicable regulatory approvals – here is the default sentence to use for standards that should become effective as soon as possible:

First day of first calendar quarter after applicable regulatory approval (or, in those jurisdictions where regulatory approval is not required, the standard becomes effective on the first day of the first calendar quarter after BOT adoption.)

Performance Requirements
Does this reliability standard state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest?

Does each requirement identify who shall do what under what conditions and to what outcome?

Fill-in-the-blank Requirements
Do not include any 'fill-in-the-blank' requirements. These are requirements that assign one entity responsibility for developing some performance measures without requiring that the performance measures be included in the body of a standard – then require another entity to comply with those requirements.

Every reliability objective can be met, at least at a threshold level, by a North American standard. If we need regions to develop regional standards, such as in under-frequency load shedding, we can always write a uniform North American standard for the applicable functional entities as a means of encouraging development of the regional standards.

Requirements for Regional Reliability Organization
Do not write any requirements for the Regional Reliability Organization. Any requirements currently assigned to the RRO should be re-assigned to the applicable functional entity. If the requirement can only be performed at a regional level, assign the requirement to the Regional Entity, not the RRO.

Violation Risk Factors
Each requirement must have an associated Violation Risk Factor (VRF). Avoid assigning a VRF to sub-requirements. If a sub-requirement needs a VRF that is different from the VRF assigned to the main requirement, then consider sub-dividing the requirement into multiple requirements. The VRF identifies the reliability-related risk of violating a requirement.

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures;

or a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures;

or a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system.

A requirement that is administrative in nature~~;~~

~~or~~ and is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to

adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

Time Horizon
The drafting team should also indicate the time horizon available for mitigating a violation to the requirement using the following definitions:

- **Long-term Planning** — a planning horizon of one year or longer.
- **Operations Planning** — operating and resource plans from day-ahead up to and including seasonal.
- **Same-day Operations** — routine actions required within the timeframe of a day, but not real-time.
- **Real-time Operations** — actions required within one hour or less to preserve the reliability of the bulk electric system.
- **Operations Assessment** — follow-up evaluations and reporting of real time operations.

Measurability
Is each performance requirement stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement?

Does each performance requirement have one or more associated measures used to objectively evaluate compliance with the requirement? Measures should comply with the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" reference document.

If performance results can be practically measured quantitatively, are metrics provided within the requirement to indicate satisfactory performance?

Violation Severity Levels
The drafting team should indicate a set of violation severity levels that can be applied for the requirements within a standard. ('Violation severity levels' replace existing 'levels of non-compliance.') The violation severity levels must be applied for each requirement and may be combined to cover multiple requirements, as long as it is clear which requirements are included and that all requirements are included.

The violation severity levels should be based on the following definitions and the latest version of the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards":

- **Lower: mostly compliant with minor exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more minor details.
- **Moderate: mostly compliant with significant exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more significant elements.
- **High: marginal performance or results** — The responsible entity has only partially achieved the reliability objective of the requirement and is missing one or more significant elements.
- **Severe: poor performance or results** — The responsible entity has failed to meet the reliability objective of the requirement.

Compliance Enforcement Authority

Replace, 'Regional Reliability Organization' with 'Regional Entity'
Replace, 'NERC' with 'ERO'
In situations where the Regional Entity is the responsible entity, or where a responsible entity works for the Regional Entity, the Compliance Enforcement Authority is the ERO. In all other situations, the Regional Entity is the Compliance Enforcement Authority.

Compliance Monitoring Period and Reset Timeframe
In all cases, enter, 'Not applicable.' (These terms are associated with an older version of the sanctions table. The next time the Reliability Standards Development Procedure is updated, the procedure will be revised to omit references to 'compliance monitoring period' and 'reset timeframe'.)

Data Retention
Use the data retention periods proposed in the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" document unless there is a justifiable reason for proposing other data retention periods.

Compliance Monitoring Processes
The list of compliance monitoring processes used with each standard should comply with the proposed list of processes identified in the "Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards" reference document. In the standard, list the compliance monitoring processes under 'Additional Compliance Information.'

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Periodic Data Submittals
- Exception Reporting
- Complaints

Associated Documents
We will delay populating this section of the standard with a list of 'related' standards because standards are all being changed and many will have new numbers. We should limit the references to those support documents that are useful in complying with the standard.

Functional Model Version 3
Review the requirements against the latest descriptions of the responsibilities and tasks assigned to functional entities as provided in pages 13 through 53 of the draft Functional Model Version 3.

Completeness
Is this reliability standard complete and self-contained? Does the standard depend on external information to determine the required level of performance?

Clear Language
Is the reliability standard stated using clear and unambiguous language? Can responsible entities, using reasonable judgment and in keeping with good utility practices, arrive at a consistent interpretation of the required performance?

Consistent Terminology
To the extent possible, does this reliability standard use a set of standard terms and definitions that are approved through the NERC reliability standards development process?

If the standard uses terms that are included in the NERC Glossary of Terms Used in Reliability Standards, then the term must be capitalized when it is used in the standard. New terms should not be added unless they have a 'unique' definition when used in a NERC reliability standard. Common terms that could be found in a college dictionary should not be defined and added to the NERC Glossary.

Practicality
Does this reliability standard establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter?

Consequences for Noncompliance
In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, are the consequences of violating a standard clearly known to the responsible entities?

Attachment 2 (this is a large attachment and is in a self-contained file)

Attachment 3

Stakeholder Issues and Recommendations Identified During Initial SAR Posting

Industry Education

- Consider what to do with the existing FAQ document e.g., modify, replace.
- Consider how to provide additional guidance in support of these standards, e.g., Technical Reference documents, guidelines, white papers.
- Consider development of a guideline document to address extended LANs over multiple geographically dispersed locations.

Balloting and Implementation

- Determine the timing and grouping of revisions to be submitted to industry for comment and ballot, e.g., multi-phase or other approach.
- Determine the optimum implementation plan for revised CIP standards in this project.
- Address when newly identified critical assets or critical cyber assets, newly acquired equipment or assets, etc. must come into compliance with CIP standards.
- Address compliance issue where internal requirements exceed NERC requirements. Clarify in view of language contained in FERC Order 706 paragraph 377.

Clarify Existing Requirements

- Consider the need for different requirements for different environments e.g., control center, substation and generation plant.
- Clarify how serial and wireless devices are subject to these standards. Refer to pp 278 and 285 of FERC Order 706.

Other Issues

- Consider issues surrounding protection of data in motion.
- Consider the issue of hybrid devices that use both serial and routable protocols.
- Consider the issue of data versus information (electronic and/or hardcopy lists, drawings, etc.) protection including transport and transmittal of such information.
- Consider a clearly defined set of risks which can result in a more focused and effective set of compliance expectations.
- With regard to third-party vendors and contractors, provide clarification and additional guidance as to how much a responsible entity may rely on the processes and procedures of contractors and vendors that support the critical infrastructure of that responsible entity under the CIP standards and still be compliant with the standard.

Standards Development
Guideline Development
ERO Staff/Process
Items of Note

Order 706

Commission Determination Statements

24. The Commission approves the eight CIP Reliability Standards pursuant to section 215(d) of the FPA, as discussed below. In approving the CIP Reliability Standards, the Commission concludes that they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. These CIP Reliability Standards, together, provide baseline requirements for the protection of critical cyber assets that support the nation's Bulk-Power System. Thus, the CIP Reliability Standards serve an important reliability goal. Further, as discussed below, the CIP Reliability Standards clearly identify the entities to which they apply, apply throughout the interconnected Bulk-Power System, and provide a reasonable timetable for implementation.

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

26. With regard to WIRAB's recommendation, we share the ongoing concern of promoting coordinated action on Reliability Standards on an international basis. However, in this instance, we do not believe a remand to NERC, which would result in significant delays in having mandatory and enforceable cyber security requirements in effect in the United States, is justified or would further such coordination. The implementation schedule provided by NERC, which applies continent-wide, requires applicable entities to achieve "auditable compliance" no earlier than mid-2009. This should provide adequate time for entities responsible for compliance with the CIP Reliability Standards in the United States, Canada and Mexico to achieve compliance on a common timetable. As discussed later, future modifications to the CIP Reliability Standards developed pursuant to the direction provided in the Final Rule would not overlap with the NERC implementation plan. Accordingly, the Commission concludes that this is not a satisfactory reason for remanding the CIP Reliability Standards.

27. In approving the CIP Reliability Standards and directing the ERO to modify them, the Commission is taking two independent actions and does not condition our approval on the ERO modifying the CIP Reliability Standards. First, we are exercising our authority to approve a proposed Reliability Standard. Second, we are directing the ERO to submit a modification of the Reliability Standards to address specific issues or concerns. Accordingly, New York Commission's concerns about the Commission placing any conditions on its approval of the CIP Reliability Standards are unnecessary.

28. With regard to the concerns raised by some commenters about the prescriptive nature of the Commission's proposed modifications, the Commission agrees that a direction for modification should not be so overly prescriptive as to preclude the consideration of viable alternatives in the ERO's Reliability Standards development process. However, in identifying a specific matter to be addressed in a modification to a CIP Reliability Standard, it is important that the Commission provide sufficient guidance so that the ERO has an understanding of the Commission's concerns and an appropriate, but not necessarily exclusive, outcome to address those concerns. Without such direction and guidance, a Commission proposal to modify a CIP Reliability Standard might be so vague that the ERO would not know how to adequately respond.

29. Thus, in some instances, while we provide specific details regarding the Commission's expectations, we intend by doing so to provide useful guidance to assist in the Reliability Standards development process, not to impede it. We find that this is consistent with statutory language that authorizes the Commission to order the ERO to submit a modification "that addresses a specific matter" if the Commission considers it appropriate to carry out section 215 of the FPA. In the Final Rule, we have considered commenters' concerns and, where a directive for modification appears to be determinative of the outcome, the Commission provides flexibility by directing the ERO to address the underlying issue through the Reliability Standards development process without mandating a specific change to the CIP Reliability Standard. Further, the Commission clarifies that, where the Final Rule identifies a concern and offers a specific approach to address that concern, we will consider an equivalent alternative approach provided that the ERO demonstrates that the alternative will adequately address the Commission's underlying concern or goal as efficiently and effectively as the Commission's proposal.

30. Consistent with section 215 of the FPA, our regulations, and Order No. 693, any modification to a Reliability Standard, including a modification that addresses a Commission directive, must be developed and fully vetted through NERC's Reliability Standard development process. Until the Commission approves NERC's proposed modification to a Reliability Standard, the preexisting Reliability Standard will remain in effect.

47. The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance with the CIP Reliability Standards. The Commission maintains its belief that NERC's compliance is necessary in light of its interconnectivity with other entities that own and operate critical assets. Further, we conclude that NERC's Rules of Procedure, which state that the ERO will comply with each Reliability Standard that identifies the ERO as an applicable entity, provides an adequate means to assure that NERC is obligated to comply with the CIP Reliability Standards. Likewise, the delegation agreements between NERC and each Regional Entity expressly state that the Regional Entity is committed to comply with approved Reliability Standards. Based on these provisions, we find that the Commission has authority to oversee the compliance of NERC and the Regional Entities with the CIP Reliability Standards.

48. With regard to EEI's concerns about NERC's incentives to comply with the CIP Reliability Standards, we believe that NERC's position as overseer of Bulk-Power System reliability provides a level of assurance that it will take compliance seriously. Moreover, section 215(e)(5) of the FPA provides that the Commission may take such action as is necessary or appropriate against the ERO or a regional entity to ensure compliance with a Reliability Standard or Commission order.

49. The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards. We are concerned, like the California Commission, that some small entities that are not identified in the NERC registry may become gateways for cyber attacks. However, we are not prepared to adopt California Commission's suggested approach of requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry. We believe this approach is overly-expansive and may raise jurisdictional issues. Rather, we rely on NERC and the Regional Entities to be vigilant in assuring that all appropriate entities are registered to ensure the security of the Bulk-Power System.

50. With regard to EEI's request for clarification, the NERC registry process is designed to identify and register entities for compliance with Reliability Standards, and not identify lists of assets. In the CIP NOPR, the Commission explained that it would expect NERC to register the owner or operator of an important asset, such as a blackstart unit, even though the facility may be relatively small or connected at

low voltage. While the facility would not be registered or listed through the registration process, NERC's or a Regional Entity's awareness of the critical asset may reasonably result in the registration of the owner or operator of the facility.

51. Likewise, we believe that NERC should register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System. EEI and ISO/RTO Council concur that the need for the registration of demand side aggregators may arise, but state that it is not clear whether aggregators fit any of the current registration categories defined by NERC. We agree with EEI and ISO/RTO Council that NERC should consider whether there is a current need to register demand side aggregators and, if so, to address any related issues and develop criteria for their registration.

52. The Commission agrees with the many commenters that suggest that the responsibility of a third-party vendor for compliance with the CIP Reliability Standards is a matter that should be addressed in contracts between the registered entity that is responsible for mandatory compliance with the Standards and its vendor. To the extent that the responsible entity makes a business decision to hire an outside contractor to perform services for it, the responsible entity remains responsible for compliance with the relevant Reliability Standards. Thus, it is incumbent upon the responsible entity to assure that its third-party vendor acts in compliance with the CIP Reliability Standards. We agree with ISO/RTO Council's characterization of the matter:

> . . . when an application is developed and maintained by an outsourced provider, that outsourced provider manages physical and cyber access to the environment on which the application runs and therefore must be contractually obligated to the Responsible Entity to comply with the Reliability Standards. While such providers are not registered entities subject to the Reliability Standards, they must perform the services and operate the applications in a manner consistent with the Reliability Standards. . . the Responsible Entity should be charged with incorporating contractual terms and conditions into agreements with third-party service providers that obligate the providers to comply with the requirements of the Reliability Standards. In that regard, if a Responsible Entity determines that it is necessary to outsource a service that is essential to the reliable operation of a Critical Asset, Critical Cyber Asset, or the bulk electric system, it is clear that the Responsible Entity must be held responsible and accountable for compliance with the Reliability Standards.

53. Further, it is incumbent upon a responsible entity to conduct vigorous oversight of the activities and procedures followed by the vendors they employ. Thus, we expect a responsible entity to address in its security policy under CIP-003-1 its policies regarding its oversight of third-party vendors.

61. The Commission received comments on both sides of the issue of specificity. Some commenters caution against the CIP Reliability Standards being too specific, while others request more guidance to help them comply. In general, the Commission believes it is appropriate to provide sufficient guidance to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. The Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. Therefore, in several instances throughout this Final Rule, the Commission gives the ERO direction to provide additional guidance. In some cases, we require that the guidance be placed in modifications to the CIP Reliability Standards. In other cases, we note that some or all of the additional guidance could be placed in a reference document separate from the CIP Reliability Standards.

62. Some of the more specific directives in this Final Rule pertain to issues that the Commission considers necessary to carry out its statutory responsibilities. Examples of this include areas of oversight, exceptions to Requirements, and reports to the Commission. In developing these directives, we have tried to strike a balance between our needs to implement the statute and the concerns expressed by commenters.

63. We agree in general with commenters who point out that compliance issues should be determined in audits and that a strong auditing process will help to ensure quality control and consistency in the implementation of the CIP Reliability Standards. However, we point out that audits are only one aspect of the ERO's compliance monitoring and enforcement process. All aspects of that process must function well. In addition, we note compliance audits are conducted after-the-fact and do not diminish the necessity for internal and external reviews of compliance efforts, including the identification of critical assets and critical cyber assets.

64. In response to Northern Indiana, we explain "external oversight" in our discussions and determinations of specific Requirements in the Final Rule.

72. While the Commission agrees with commenters that relying on an objective determination such as whether a document exists would facilitate the compliance audit process, we do not believe such a cursory approach is the best way to ensure the protection of the Bulk-Power System. We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement. In this way we affirm the Commission's position established in Order No. 693 that, "while Measures and Levels of Non-Compliance provide useful guidance to the industry, compliance will in all cases be measured by determining whether a party met or failed to meet the Requirement given the specific facts and circumstance of its use, ownership or operation of the Bulk- Power System." While we agree with Northern Indiana that, depending on the Requirement in question, in some instances (such as active system testing) documentation would suffice to demonstrate compliance, even in these cases auditors should look at the content of the documentation to determine if the substance of the Requirement has been met.

73. Xcel seeks clarification regarding responsible entities that comply with the substance of a Requirement but violate the documentation provisions. In Order No. 693, in response to a similar request by Xcel, the Commission explained that, "[w]hile the Commission generally agrees that it is a violation of the Requirements that is subject to a penalty, we recognize that because Measures are intended to gauge or document compliance, failure to meet a Measure is almost always going to result in a violation of a Requirement." We add that a responsible entity's failure to maintain documentation (as set forth in a Measure) that obstructs the ability of the ERO, Regional Entity or Commission to determine compliance with the substance of a Requirement may warrant a penalty.

74. In the CIP NOPR, the Commission also noted that, while certain Requirements of the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, the Requirements do not always explicitly require implementation of the plan, policy or procedure. The Commission proposed to interpret such provisions to include an implicit implementation requirement.

75. Consistent with that proposal, the Commission concludes that, where the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, there should be a corresponding obligation to implement the plan, policy or procedure. However, while the CIP NOPR proposed to interpret the CIP Reliability Standards as including an implicit obligation to implement plans, policies and procedures, we are persuaded by the commenters that a better approach is for the ERO to

develop modifications to the CIP Reliability Standards that contain appropriate implementation language. Accordingly, we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards.

76. As to Xcel's argument that, at times, the proper course is to deviate from a plan, we agree that the details of such plans are not equivalent to Requirements of a CIP Reliability Standard. However, the responsible entity's plan should be followed unless a deliberate decision is made for good reason not to follow it. Such reason should be documented and available for compliance auditors to review. Merely ignoring plan provisions is equivalent to not having a plan. For clarity, we note that a decision not to follow a particular plan provision due to circumstances will not except a responsible entity from a related Requirement in a CIP Reliability Standard. As discussed below, we find that any exception to a CIP Reliability Standard must comply with the required conditions for a technical feasibility exception.

77. In the CIP NOPR, the Commission explained that, because the CIP Reliability Standards are new and require applicable entities in many cases to develop new cyber security systems and procedures, NERC developed an implementation plan based on a schedule that provides for implementation of the CIP Reliability Standards over a three year period. The implementation plan sets out a proposed schedule for accomplishing the various tasks associated with compliance with the CIP Reliability Standards. The schedule gives a timeline by calendar quarters for completing various tasks and prescribes milestones for when a responsible entity must: (1) "begin work;" (2) "be substantially compliant" with a Requirement; (3) "be compliant" with a Requirement; and (4) "be auditably compliant" with a Requirement. According to the implementation plan, "auditably compliant" must be achieved in 2009 for certain Requirements by certain responsible entities, and in 2010 for others

86. The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities to achieve auditable compliance. Responsible entities require a reasonable period of time to purchase and install new cyber software and equipment and develop new programs and procedures to achieve compliance. Commenters indicate that the implementation plan provides that reasonable period of time. Further, we agree with commenters that there is an urgent need to move forward without any delays. Accordingly, we approve NERC's implementation plan.

87. Commenters raise concerns regarding the impact on the implementation plan of the Commission's directives for modifications to the CIP Reliability Standards. As explained above, the Commission is not modifying the CIP Reliability Standards in this Final Rule. Rather, pursuant to section 215(d)(5) of the FPA, the Commission in the Final Rule directs the ERO to develop certain modifications to the CIP Reliability Standards pursuant to the NERC Reliability Standards development process. Even though the development of such modifications will take time, this does not present a reason for delay or revision to the NERC implementation plan for implementing the CIP Reliability Standards approved in this Final Rule.

88. The Commission believes that the modifications to the CIP Reliability Standards developed by the NERC Reliability Standards development process should not be audited prior to the conclusion of the approved implementation plan. EEI and other commenters claim that commencing the development of such modifications prior to the conclusion of the implementation plan would be discouraging to industry. The Commission, however, finds that it is unacceptable to delay the development of the modifications directed in this Final Rule until after the conclusion of the implementation plan. Since it is uncertain how long it will take to develop revised CIP Reliability Standards, we believe it is not reasonable to wait until the 2009-2010 time period for the process to start. Features such as enhanced conditions on technical

feasibility exceptions and oversight of critical asset determinations are too important to the protection of the Bulk-Power System to wait that long.

89. While we are both sympathetic and concerned about straining industry resources, the Commission and the electric industry must do their best to protect the electric infrastructure that is essential to the health and safety of the nation. Therefore, we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule. As suggested by NERC, the Commission will consider a second implementation plan for achieving compliance with the forthcoming revised CIP Reliability Standards.

90. The Commission did not propose to remand CIP-002-1 as argued by Entergy. Nonetheless, Entergy raises a valid concern since the Commission's directive, discussed below, that the ERO develop modifications to CIP-002-1 could affect a responsible entity's identification of critical assets. We share Entergy's concern that there are threshold issues regarding CIP-002-1 that must be addressed before responsible entities can have certainty regarding which assets must be protected according to the CIP Reliability Standards. We also believe that responsible entities need certainty regarding the conditions for a technical feasibility exception to inform their decisions about how to comply with the CIP Reliability Standards, even in their current form. Therefore, we direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.

96. While the Commission is sensitive to concerns that more frequent self certifications may be burdensome, it is important that the ERO and the Commission know whether industry, or segments of industry, are having difficulty implementing the CIP Reliability Standards. Therefore, we direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required. Such additional self-certifications may be a "stream-lined" version, but must be useful for the ERO and the Commission to assess industry's progress toward achieving compliance with the CIP Reliability Standards.

97. Further, we adopt our CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify. The ERO and the Regional Entities should then work with such an entity either informally or, if appropriate, by requiring a remedial plan to assist such an entity in achieving full compliance in a timely manner. Further, we expect the ERO and the Regional Entities to provide informational guidance, upon request, to assist a responsible entity in assessing its progress in reaching "auditably compliant" status.

98. With regard to METC-ITC's comment, we will not require NERC and the Regional Entities to submit plans describing how it will undertake these responsibilities. Rather, the ERO and Regional Entities can address any need for additional resources in the ERO's annual budget filing. If necessary to fulfill their statutory obligations, the ERO and Regional Entities may file a request for additional funding to supplement their Commission approved budgets.

99. With regard to SDG&E's comment, we clarify that the goal of a Regional Entity working with a responsible entity that is unable to self-certify is to assist the entity in meeting the NERC time frames for auditable compliance, and not to accelerate compliance ahead of schedule.

101. "NERC and other commenters oppose the addition of a cyber security assessment to NERC's existing readiness review…"

105. The Commission is persuaded by comments regarding the limited reach of readiness reviews and the questionable utility of such reviews prior to the date by which entities are to be compliant; thus, adding the CIP Reliability Standards to the readiness reviews at this time will delay industry's compliance efforts. Therefore, the Commission will not require that the CIP Reliability Standards be added to the readiness reviews at this time.

111. "…cost can be a valid consideration in implementing the CIP Reliability Standards."

128. Consistent with the CIP NOPR, the Commission concludes that the concept of reasonable business judgment is inappropriate in the context of mandatory CIP Reliability Standards. Accordingly, the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.

129. While there may have been no intention to import corporate law concepts into the CIP Reliability Standards, it is difficult to draw any other conclusion on the basis of the documents provided. We note that the only guidance on reasonable business judgment that emerged from the Reliability Standards development process and that was supplied to the Commission is found in the FAQ document, and that document appears to invoke the traditional corporate law business judgment rule. The FAQ document specifically references existing court precedent on the rule, and it sets forth the elements of reasonable business judgment in what is essentially a restatement of classic formulations of the business judgment rule. Moreover, the FAQ document specifically references one of the most objectionable aspects of the business judgment rule in the cyber security context, the requirement that the courts defer to the decisions of company officers and directors in all but the most extreme circumstances.

130. In short, the only explanation of reasonable business judgment in the documentation responsible entities would rely on focuses on corporate law concepts. We thus reject Mr. Brown's claim what we are being hyper-legalistic and constructing straw men rather than addressing the clear intent of the language. Mr. Brown fails to identify where some intent other than to adopt the traditional business judgment rule is clearly stated, and his references to 200 years of legal precedent only serve to reinforce our conclusion. We are unaware of any such extensive body of precedent on reasonable business judgment other than that developed in the corporate law context.

131. The most common argument raised in favor of reasonable business judgment is that it ensures flexibility. The Commission, however, acknowledged the importance of flexibility and discretion in the CIP NOPR. The CIP Reliability Standards consist for the most part of quite general Requirements that must be implemented in a wide variety of circumstances. As drafted, they do not provide one-size-fits-all solutions and, rather, require responsible entities to assess their individual situations and devise solutions appropriate to their circumstances. We therefore disagree with Ontario Power that outright removal of all references to reasonable business judgment would render the CIP Reliability Standards too rigid. It will still be necessary for responsible entities to choose between available alternatives to arrive at cyber security solutions that best fit their situation. In short, the CIP Reliability Standards do not simply allow flexibility, they require it.

132. Many commenters suggest that the issue is not simply flexibility, but rather the flexibility to balance costs against other factors when implementing the CIP Reliability Standards. Many of the arguments about cost have been raised in connection with the problem of technical feasibility as it relates to long-life legacy equipment. We will address that issue below and note here simply that cost is a relevant

consideration for those purposes, and recourse to reasonable business judgment is unnecessary to confirm that or to address the problem appropriately. Beyond that we disagree that deleting references to reasonable business judgment will lead to overly burdensome requirements or counterproductive results. For example, we disagree with Tampa Electric that without the leeway afforded by reasonable business judgment responsible entities would be forced into cost-prohibitive controls that do not add value in terms of security. No explanation was provided as to how this might occur. The Commission acknowledged the validity of cost considerations in the CIP NOPR and reaffirms that position here. The funds available for cyber security will not be infinite and, therefore, a responsible entity will need to make careful judgments to ensure that available funds are spent effectively. We do not see how the absence of references to reasonable business judgment will prevent this from happening.

133. Finally, some commenters link the need for flexibility with the problem of liability. We are keenly aware that unlike many other aspects of Bulk-Power System operations, cyber security represents a new and rapidly developing field. In other areas, the substance of appropriate practices is well established and well understood, but there can be considerably more uncertainty in the cyber security realm. Responsible entities therefore quite understandably wish to have, in Entergy's words, assurances that their actions meet the CIP Reliability Standards and Requirements if they act in good faith, perform the proper evaluation, and act consistent with their evaluation. We agree that they should have such assurances, but we disagree that references to reasonable business judgment are an appropriate way to provide such assurances. The real issue is whether responsible entities take reasonable and prudent actions based on an informed understanding of the current state of cyber security practice and how it applies to their situation. The Commission, therefore, disagrees with AMP-Ohio and Mr. Brown that the absence of references to reasonable business judgment will lead to a strict liability enforcement regime.

134. We disagree with Mr. Brown's claim that removal of reasonable business judgment could lead to liability for individual managers under section 215 of the FPA. That section applies to users, owners, and operators of the Bulk-Power System, and any liability arising under section 215 applies to them, not their employees.

135. Although we disagree with National Grid and others that alternative language is necessary to ensure necessary flexibility, we agree that the ERO and the participants in the Reliability Standards development process may choose to develop alternative language to replace reasonable business judgment and propose it for Commission approval. Such language would need to be adapted to the issues involved in forming judgments on proper cyber security measures and embody an objective standard focused on conduct that promotes the interests of Bulk-Power System security and reliability. Such language would also need to take into consideration our finding discussed below that a responsible entity cannot excuse itself from compliance with a requirement of the CIP Reliability Standards.

136. In response to the Southwest TDUs, we note that the CIP Reliability Standards apply in the same way to both public and private users, owners, and operators of the Bulk-Power System. Any specific issues that Southwest TDUs have with the Reliability Standards should be raised in the Reliability Standards development process.

137. Finally, we reject arguments that we are being overly prescriptive in directing the ERO to remove all references to reasonable business judgment from the CIP Reliability Standards. We discuss that general issue elsewhere in this Final Rule and will not repeat that discussion here. It is, however, important to note that such objections are inapposite in this instance for an additional reason that involves the specific nature of the issue raised. The concept of reasonable business judgment speaks to a general legal standard of conduct proposed to apply under a statute that Congress has directed the Commission to administer. It does not involve matters specific to reliability but rather is bound up with the problem of legal

enforceability. The Commission has a particular duty to see that the laws it administers can be enforced effectively. We are not being overly prescriptive when acting to ensure that this will be the case.

138. Based on the above discussion, as well as our lengthy analysis in the CIP NOPR, the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.

150. The Commission continues to view the term "acceptance of risk" as representing an uncontrolled exception from compliance that creates unnecessary uncertainty about the existence of potential vulnerabilities. Responsible entities should not be able to opt out of compliance with mandatory Reliability Standards. The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.

151. In response to concerns raised by NERC, EEI and others, we agree that this action should occur through the Reliability Standards development process. In response to the concerns of many commenters who argue that it should be possible to propose alternative language, we note that this is consistent with the Reliability Standards development process. However, any alternative language that provides a similar opportunity for a responsible entity to opt out of compliance would be subject to remand. Rather, the Commission believes that alternative language that deals with such issues in terms of technical feasibility is preferable. To that end, we have adapted the concept of technical exceptions to encompass a broader range of valid justifications. Elsewhere in this Final Rule we address the criticism that our actions are overly prescriptive and those remarks apply equally here.

152. Expanding the use of the technical feasibility conditions would address the desire for flexibility expressed by some commenters while providing the control that the Commission finds to be necessary. It would provide for documentation, reporting and approval of how responsible entities have elected to comply with the CIP Reliability Standards and thus would permit the ERO and Regional Entities to assess the significance of any possible vulnerability. As to the argument by METC-ITC that a technical feasibility exception may not be possible in all cases, we note that we have found that technical feasibility should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable. Thus, this approach addresses the issue of inadequately tested patches raised by APPA/LPPC, and similar general concerns raised by Tampa Electric.

153. In response to Entergy, we note that a long-established practice of risk acceptance by senior management does not mean that a continuation of this practice is appropriate under a new system of mandatory cyber security Reliability Standards. We have addressed Entergy's concerns about costs-related legacy equipment in connection with technical feasibility.

154. Many commenters defend retention of the acceptance of risk language by pointing out that it is impossible to eliminate all risk. While likely true, it is beside the point. The acceptance of risk language in the CIP Reliability Standards fails to acknowledge that the real issue is whether the nature and level of inevitable risk is acceptable from a systemwide perspective. Within a system of CIP Reliability Standards intended to protect the Bulk-Power System as a whole, that problem can be addressed by a system that documents and reports the risks in question and ultimately subjects them to approval by the ERO or Regional Entities. The Commission's concern in the CIP NOPR was with the lack of appropriate controls, and eliminating references to acceptance of risk does not imply that all risk can be eliminated.

155. We disagree with Mr. Brown that mutual distrust means that risks accepted by one entity do not affect others on an interconnected control system. A mutual distrust approach is a good security posture. However, its value depends on how well it is implemented. There will likely be a variety of levels of

sophistication applied to implementing mutual distrust. It is not a basis for allowing other responsible entities to ignore their obligations under mandatory CIP Reliability Standards.

156. Accordingly, the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.

178. The Commission adopts the CIP NOPR proposal and directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards. We will modify some of our proposed criteria for that framework of accountability further below. We are persuaded by commenters that the proposed conditions for invoking the technical feasibility exception should allow for operational considerations. In response to Northern Indiana and other commenters, we note that the Commission did not propose to eliminate references to technical feasibility from the CIP Reliability Standards, only that the term be interpreted narrowly and without reference to considerations of business judgment.

179. In response to those commenters who argue that the Commission's concerns and directives should be addressed through the Reliability Standards development process, we agree that to the degree revisions to the Reliability Standards are necessary to address our concerns, they would be made through that process. We disagree, however, with the arguments that claim we are rewriting the CIP Reliability Standards or adhering to a onesize- fits-all approach. With respect to the latter point, we note that technical feasibility issues are by their nature something that must be dealt with on a case-by-case basis, as they only arise in specific circumstances. Our concern here is primarily with the framework within which decisions on technical feasibility are made and ensuring that this framework promotes sound decisions that lead to effective results. The oversight provisions we describe below are essential elements of such a framework.

180. We agree with NERC and other commenters on the underlying rationale for a technical feasibility exception, i.e., that there is long-life equipment in place that is not readily compatible with a modern environment where cyber security issues are an acknowledged concern. While equipment replacement will often be appropriate to comply with the CIP Reliability Standards, such as in instances where equipment is near the end of its useful life or when alternative or supplemental security measures are not possible, we acknowledge that the possibility of being required to replace equipment before the end of its useful life is a valid concern.

181. The Commission, however, disagrees with Northern Indiana that technical feasibility should be interpreted to apply to future assets also. The justification presented for technical feasibility exceptions is rooted in the problem of long-life legacy equipment and the economic considerations involved in the replacement of such equipment before the end of its useful life. We recognize that these considerations can be valid in some cases, but Northern Indiana has not explained why technical feasibility exceptions should apply to replacement equipment. The Commission neither assumes that technical infeasibility issues will be present only during the transition period, nor does it assume that on a going forward basis there will be only one single means to comply with the CIP Reliability Standards. It does assume, however, that all responsible entities eventually will be able to achieve full compliance with the CIP Reliability Standards when the legacy equipment that creates the need for the exception is supplemented, upgraded or replaced.

182. The Commission agrees with various commenters that the implementation of the CIP Reliability Standards should not be permitted to have an adverse effect on reliability and that proper implementation requires that care be taken to avoid unintended consequences. We thus believe it is important to clarify

that the meaning of "technical feasibility" should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable.

183. We disagree with Mr. Brown's view that whether or when to replace equipment that cannot do something due to technical feasibility with equipment that can do so is purely a managerial decision, especially since he intertwines this proposition with the concept of reasonable business judgment. While we accept NERC's rationale for technical feasibility exceptions, as discussed below, an integral issue in individual cases where legacy equipment presents a technical feasibility issue is whether an alternative course of action protects the reliability of the Bulk-Power System to an equal or greater degree than compliance would. This is not a purely managerial decision involving reasonable business judgment, regardless of what meaning one imparts to that term.

184. While a number of commenters agree that it is important to clarify the meaning of technical feasibility, none appear to support defining the term in the NERC Glossary. Therefore, in light of the comments received generally and the specific guidance that we are providing to the ERO in connection with technical feasibility, we conclude that a definition of this type is unnecessary. A definition cannot substitute for a framework of conditions or criteria to provide accountability, and if those conditions or criteria are implemented, a definition is not needed. We do not agree with NERC that replacing the term technical feasibility with "exemption for reliability" would be helpful. We note, in particular, that an "exemption" normally is understood to be a release from an obligation whereas what is under discussion here is an exception that forms an alternative obligation.

185. While the Commission will not address the merits of any particular technology, we note that Teltone's comments raise an important general consideration when developing policy on technical feasibility. While technical limitations present real issues, and while one should not be overly optimistic that technological developments will resolve them sooner than expected, one should not be overly pessimistic either. Indeed, high standards should, if anything, encourage the development of technical solutions.

186. Based on the above considerations, the Commission adopts its proposal in the CIP NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place. The term technical feasibility should be interpreted narrowly to not include considerations of business judgment, but we agree with commenters that it should include operational and safety considerations

192. With some minor refinements discussed below, the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception. While the CIP NOPR proposed that each remediation plan contain a reasonable completion date, the Commission is persuaded by the comments of National Grid and SPP that a date certain for remediation may not be possible in some instances. While we expect remediation by a date certain to be the norm, we will not require a date certain for remediation in every instance that a responsible entity invokes the technical feasibility exception. An entity must provide an explanation when it believes that it is not possible for a remediation plan to provide a reasonable completion date.

193. We also agree with Northern Indiana that in some instances remediation can be required only to the extent possible. For example, in some cases it may never be possible to enclose certain critical cyber assets within a six-sided physical boundary as required under CIP-006-1. However, such cases need to be sufficiently justified, the mitigation strategies must be ongoing and effective, and the justification must be subject to periodic review. We also are mindful that accelerated replacement of equipment can be economically wasteful where security is not otherwise compromised. We thus agree with National Grid that where mitigation measures are as or more effective than compliance, and in the case of minor technical or administrative requirements, replacement of certain assets before the end of their useful lives can be wasteful and inefficient. We also agree with SPP that remediation might not be necessary where compensating measures are equally effective in reducing risk. However, such cases must be subject to clear criteria and periodic review and, where necessary, updates.

194. However, in adopting this approach, we do not intend to suggest that it would never be necessary to replace equipment before the end of its useful life to achieve cyber security goals. Where equipment is near the end of its useful life or if insufficient mitigation measures are available, the equipment should be replaced. However, such situations must be dealt with on a case-by-case basis. We emphasize that responsible entities must protect assets that are critical to the reliable operation of the Bulk-Power System.

209. For the reasons discussed below, the Commission concludes that technical feasibility exceptions should be reported and justified and subject to approval by the ERO or the relevant Regional Entity. The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria. However, because we are persuaded by the commenters, we have modified certain elements of our original proposal, as discussed below.

210. Most objections to the CIP NOPR proposal regarding the review and approval of technical feasibility exceptions are not objections in principle but rather focus on practical issues of implementation, such as limited ERO and Regional Entity resources and sensitivity of the information in question. To the extent that objections in principle have been raised, we disagree. Thus, we disagree with ReliabilityFirst's argument that senior manager approval of exceptions is unnecessary because of the responsibilities already assigned to the senior manager by CIP-003-1. These technical feasibility exceptions implicate matters that go beyond the purview of individual responsible entities and must be subject to review and approval by those with a wider-area view and general responsibility for system reliability. We also disagree with the ISO/RTO Council that the Commission should simply direct the ERO to detail the type of justifications and considerations that must be documented when invoking a technical feasibility exemption. While such guidance could be useful, it cannot substitute for reporting, review, and approval, which is necessary to address concerns that extend beyond the reach of an individual responsible entity.

211. With regard to the senior management approval, we continue to believe that internal approval is an important component of an overall framework of accountability with regard to use of the technical feasibility exception. Therefore, we adopt this aspect of our CIP NIPR proposal and direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.

212. However, the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed. We agree, in particular, with those commenters who argue that pre-approval could tax ERO and Regional Entity resources, delay implementation, and possibly create undue risks that sensitive information will be disclosed.

213. The Commission agrees with National Grid that Regional Entities should, in the first instance, receive and catalogue notices of technical feasibility exceptions that are claimed. Such notices must include estimates of the degree to which mitigation measures achieve the goals set by a CIP Reliability Standard and be in sufficient detail to allow verification of whether reliance on exceptions (or the associated mitigation measures) adequately maintains reliability and does not create reliability issues for neighboring systems. Initial submission of notices should be provided by responsible entities at least by the "Compliant" stage of implementation in order to allow Regional Entities to plan for auditing exceptions, as described in more detail below.

214. The Commission also agrees with National Grid, EEI and others that actual evaluation and approval of technical feasibility exceptions should be performed in the first instance in the audit process. This would allow assessment of exceptions within their specific context and thus facilitate greater understanding in evaluating individual exceptions, as well as related mitigation steps and remediation plans. This also would increase the amount of sensitive information that remains on-site and reduces the risk of improper disclosure. In addition, it will allow the ERO and Regional Entities, informed by the initial notices discussed above, to include personnel in audit teams with sufficient expertise to judge the need for a technical feasibility exception and the sufficiency of preferred mitigation measures.

215. Given the significance of technical feasibility exceptions, the Commission believes that initial audits of technical feasibility exceptions should be expedited, i.e., performed earlier than otherwise, including moving the audit to an earlier year. Also, in general, responsible entities claiming such exceptions should receive higher priority when determining which entities to audit, and the more exceptions an entity has, the higher the priority for audit should be. Further, NERC may provide an appeals process for the review of technical feasibility exceptions, if it determines that this is appropriate.

216. However, the Commission notes that the audit process is a Regional Entity and ERO process, and audit team findings regarding exceptions are subject to Regional Entity and ERO review. The Commission believes that the audit report should form the basis for ERO or Regional Entity approval of individual exceptions. Approval thus represents a determination on compliance with the applicable CIP Reliability Standards, and we disagree with the ISO/RTO Council that approval of technical feasibility exceptions raises any conflict of interest or due process concerns. The proposed procedures raise no special issues in this respect.

217. We agree with EEI and others that approvals and potential appeals should not be allowed to delay implementation, but we believe our revised proposal resolves this problem. We also agree with APPA/LPPC that responsible entities should be able to rely on a technical feasibility exception prior to formal approval. However, we disagree with Northern Indiana that penalties should be waived within the time when an approved remediation plan is being implemented, as proper implementation of the plan itself constitutes a necessary element of compliance.

218. In summary, on the issues pertaining to external approval of a responsible entity's use of the technical feasibility exception, rather than a pre-approval process, we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process. This process should require the ERO or a Regional Entity to approve any technical feasibility exception, taking into account whether the technical feasibility exception is needed and whether the mitigation and remediation steps are adequate to the circumstance.

219. We agree with comments emphasizing the importance of protecting sensitive information relating to technical feasibility exceptions. We agree with SPP and others that CEII treatment should be available for

any such information. In response to Bonneville, we agree that a governmental entity subject to FOIA requirements should not be required to submit sensitive information about critical assets or critical cyber assets that could be deemed a waiver of FOIA protection that is otherwise available. Nonetheless, a governmental entity's decision to rely on a technical feasibility exception should also be subject to appropriate oversight and accountability. Thus, we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive information.

220. As stated in the CIP NOPR, the Commission believes that it is important that the ERO, Regional Entities and the Commission understand the circumstances and manner in which responsible entities invoke the technical feasibility exception. Accordingly, we direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability. The annual report must address, at a minimum, the frequency of the use of such provisions, the circumstances or justifications that prompt their use, the interim mitigation measures used to address vulnerabilities, and efforts to eliminate future reliance on the exception.

221. While we agree with commenters that the compilation of data for the annual report must not compromise the security of the Bulk-Power System, we disagree that this is a reason not to require the report. Rather, as we indicated in the CIP NOPR, the report should not provide a level of detail that divulges CEII data. Rather, the report should contain aggregated data with sufficient detail for the Commission to understand the frequency with which specific provisions are being invoked as well as high level data regarding mitigation and remediation plans over time and by region. Further, we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.

222. In conclusion, pursuant to section 215(d)(5) of the FPA, we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards. As discussed above, structural elements of this framework include mitigation steps, a remediation plan, a timeline for eliminating use of the technical feasibility exception unless appropriate justification otherwise is provided, regular review of whether it continues to be necessary to invoke the exception, internal approval by the senior manager, wide-area approval through the ERO's audit process, and cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding the effects the technical feasibility exception on the reliability of the Bulk-Power System. We direct the ERO to develop appropriate modifications, as discussed above.

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe – and is further persuaded by the comments – that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability

Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.

236. … the commission approves Standard CIP-002-1 as mandatory and enforceable.

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

254. Commenters raise a number of topics that they believe should be addressed in the NERC guidance, such as how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary. We believe these are all appropriate topics to be addressed and direct the ERO to consider these commenter concerns when developing the guidance.

255. The Commission proposed in the CIP NOPR that the ERO and Regional Entities provide reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical because, for example, the impact of the facility may be dependent on their connection with a transmission owner or operator. While we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.

256. Regarding MidAmerican's comments on use of the N minus 1 criterion when applying a risk-based assessment methodology to the identification of critical assets, we agree with MidAmerican that an N minus 1 criterion is not an appropriate risk-based assessment methodology for identifying critical assets. While the N minus 1 criterion may be appropriate in transmission planning, use of an N minus 1 criterion for the risk based assessment in CIP-002-1 would result in the nonsensical result that no substations or generating plants need to be protected from cyber events. A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset. Also, we note that the definition of "critical assets" is focused on the criticality of the asset, not the likelihood of an outage. Based on this reasoning, in response to US Power, we clarify that a generator

should not assume that none of its individual generating assets would be regarded "critical" to the Bulk-Power System.

> **Footnote 84: Further, Requirement R.1.2.3 provides that the risk-based assessment must consider "generation resources that support the reliable operation" of the Bulk-Power System. This language indicates that certain generation facilities, and presumably some facilities within a region identified as critical, must be considered in an assessment. Beyond this, we leave it to the ERO to provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset. As discussed later in the Final Rule, the Commission will monitor and evaluate the outcome of this endeavor – the list of critical assets.**

257. With regard to Xcel's request for clarification regarding the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4, we direct the ERO to consider this clarification in its Reliability Standards development process.

258. As to Entergy's suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Likewise, the ERO should consider Northern California's suggestion that the ERO establish a formal "feedback loop" to assist the industry in developing policies and procedures.

270. As discussed above, commenters that address the subject uniformly oppose the CIP NOPR statement that "marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process the data, would be considered critical cyber assets" subject to the CIP Reliability Standards. These commenters contend that marketing data typically does not qualify as a critical cyber asset and the Commission's proposal is beyond the current scope of the CIP Reliability Standards. Moreover, several commenters suggest that some data and support systems may fit the definition of critical asset and, thus, supporting critical cyber assets must comply with CIP-002-1.

271. The Commission remains concerned that, while not all marketing data or other data may be considered a critical cyber asset essential to the proper operation of a critical asset, there may be times where it is properly classified as such. For example, if a critical asset is configured such that it cannot operate and support the reliability and operability of the Bulk-Power System without a real-time stream of data, that data fits the definition of a critical cyber asset, and should be protected. Once a particular piece of data is no longer needed by the critical asset, it is no longer a critical cyber asset. On this point, we agree with commenters that there is a temporal characteristic to data as a critical asset.

272. Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.

273. The Commission also agrees with ISO-NE that experience in the implementation of the CIP Reliability Standards may indicate a need to further address this topic in a future proceeding.

279. The Commission accepts the explanation of the ERO and ReliabilityFirst that a control system could be a critical cyber asset, but not a critical asset.

280. The Commission has two concerns regarding the misuse of facilities, and clarifies those concerns here. First, Requirement R1.2.1 requires responsible entities to consider control centers and backup control centers as potential critical assets. In determining whether those control centers should be critical assets, we believe that responsible entities should examine the impact on reliability if the control centers are unavailable, due for example to power or communications failures, or denial of service attacks. Responsible entities should also examine the impact that misuse of those control centers could have on the electric facilities they control and what the combined impact of those electric facilities could be on the reliability of the Bulk-Power System. The Commission recognizes that, when these matters are taken into account, it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset.

281. Second, the Commission is concerned about the misuse of a control system that controls more than one asset. The assets could be multiple generating units, multiple transmission breakers, or perhaps even multiple substations. All of the controlled assets could be taken out of service simultaneously due to a failure or misuse of the control system. Individually, perhaps none of the controlled assets would be considered as a critical asset. However, with a simultaneous outage due to the single point of control, the controlled assets might affect the reliability or operability of the Bulk-Power System and, therefore, should be considered as critical assets. In that case, the common control system should be considered a critical cyber asset.

282. Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets. The clarification of our concern over misuse of control systems addresses Entergy's comment on this issue as well.

283. The Commission concurs with SPP that both insider and external threats should be considered as part of a risk-based assessment.

284. We share Applied Control Solutions' concern that too few assets may be identified as critical cyber assets. However, there is no evidence that will be the case, and there is no formally accepted method for identifying critical cyber assets before us at this time. Therefore, we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time. The Commission may revisit this circumstance in a future proceeding.

285. As to the conflicting comments of ISA99 Team and Energy Producers, Requirement R2 of CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial-up access. Energy Producers argues that Requirement R2 should be retained, while ISA99 Team argues that devices that use non-routable protocols should also be considered as possible critical cyber assets. We do not find sufficient justification to remove this provision at this time. However, we direct the ERO to consider the comment from ISA99 Team. We also do not find sufficient justification to order the inclusion of communication links in CIP-002-1 at this time.

288. To clarify, the Commission did not propose to direct that the ERO develop a requirement for responsible entities to document why each specific asset was identified or not identified as "critical." Rather, the Commission's intent was that a responsible entity must be able to explain such

determinations, for example upon inquiry by an auditor, to confirm compliance with the Reliability Standard. Nonetheless, we are persuaded by the commenters that the documentation of a responsible entity's risk-based assessment methodology pursuant to Requirement R1.1 and the results of its annual application of the methodology pursuant to Requirement R2 should suffice to explain a responsible entity's asset determinations. Accordingly, the Commission will not direct the ERO to develop a modification to address this concern. However, if experience shows that responsible entities are failing to consider in their assessments specific types of assets that the Commission, ERO or others believe should be included in an assessment and therefore not in compliance with the Reliability Standard, there may be a need to revisit this matter in the future.

294. The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology. This determination is consistent with the Blackout Report's recommendation to establish clear authority and ownership for physical and cyber security. Further, regardless of whether the current Requirements implicitly require senior manager review of the assessment methodology, we believe the matter is too important to rely on inference. Accordingly, the Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.

295. With regard to Northern Indiana's concerns, we are not directing a revision to the current language of Requirement R4 which provides for "the senior manager or delegate(s)'s approval" of the list of critical assets and list of critical cyber assets. As we understand the provision, the senior manager still retains ultimate responsibility for the determinations of his or her delegate(s). Otherwise, senior management could avoid responsibility by 'delegating downward.'

296. With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."

297. In response to comments by Bonneville and NRECA, the Commission clarifies that we do not intend that an individual employee of a user, owner or operator of the Bulk-Power System will be subject to a penalty pursuant to section 215 of the FPA because a responsible entity violates a CIP Reliability Standard. This matter is addressed in more detail in our discussion of CIP-003-1.

319. The Commission affirms its CIP NOPR determination that responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR, and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities - both small and large - in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility.

320. We will not allow a "safe harbor" for good faith compliance as requested by AMP Ohio. We do not believe that blanket waivers from an enforcement action are appropriate in this context and have

previously denied other requests for safe harbors from enforcement. Rather, we believe that demonstrable good faith compliance is a legitimate mitigating factor in an enforcement action.

321. SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system.

322. The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists. The Commission finds that an external review of critical assets by an appropriate organization is needed to assure that such lists are considered from a wide-area view (i.e., from a regional perspective) and to identify trends in critical asset identification. Further, while we recognize that individual circumstances may likely vary, an external review will provide an appropriate level of consistency.

323. The Commission disagrees with the suggestion of Luminant and others that external review should be voluntary. The identification of critical assets pursuant to CIP- 002-1 is crucial to cyber security protection because this determination controls whether a responsible entity must comply with the remaining CIP requirements in CIP-003-1 through CIP-009-1. External review will help ensure that responsible entities have an accurate and complete list of critical assets, which will in turn allow them to be appropriately protected to further the security of the nation's Bulk-Power System. Allowing external review as a voluntary measure is not adequate to ensure that responsible entities are prepared to address cyber vulnerabilities and cyber threats. Based on the same reasoning, we reject the suggestion of Northern Indiana and others that the external review should only address the assessment methodology, and not critical asset lists.

324. The Commission also disagrees with commenters who insist that the external review can be performed pursuant to the ERO's and Regional Entity's current compliance and enforcement programs, and the audit process in particular. While the Commission decided earlier in the Final Rule to rely on the ERO and regional audit processes to examine exceptions to compliance based on "technical feasibility," the Commission does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations. Review of critical asset lists through individual audits would span a significant period of time, measured in years, during which time such lists would not undergo review and possibly gaps in security could result. While EEI's suggestion of spot checks prior to the "auditably compliant" stage would provide more timely feedback it would, by design, not be comprehensive. The Commission concludes that a structured program for the formal, timely review of critical assets lists is a reasonable means to provide timely, comprehensive guidance to responsible entities on the adequacy of their critical asset lists.

325. The Commission agrees with Ontario IESO that in a dispute between a responsible entity and the external reviewer over whether to identify an additional asset as critical, the external reviewer should prevail. (However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets.) We recognize, however, that there may be a legitimate reason for a responsible entity to dispute such a determination, possibly through an appeal. We leave it to the ERO to determine the need for such an appeal mechanism and, if appropriate, the development of appropriate procedures (or reliance on appeal procedures currently provided in the NERC Rules of Procedure). While the ERO may determine

that an appeals process is a necessary aspect of this program, we do not believe that the burden of such appeals outweighs the benefits of the external review of critical asset lists.

326. The Commission in the CIP NOPR proposed that the Regional Entities be responsible for the external review of critical asset lists, and also expressed a willingness to consider a review process that allows for the participation of other organizations such as reliability coordinators and transmission planners. As indicated above, a number of commenters question whether the Regional Entities have the expertise or resources to conduct the reviews. Rather, there was considerable support for reliability coordinators conducting the external review because of their technical expertise, their wide-area view and their role of coordinating among neighboring systems.

327. The Commission believes that the Regional Entities must have a role in the external review to assure that there is sufficient accountability in the process. Further, a Regional Entity role is necessary because the Regional Entities and ERO are ultimately responsible for ensuring compliance with Reliability Standards. For example, if the ERO determines that an appeals process is needed, this process cannot rest with an active owner or operator of the Bulk-Power System such as a reliability coordinator. Moreover, the ERO and the Commission have oversight authority of the Regional Entities' programs and procedures pursuant to section 215 of the FPA.

328. Beyond the direction that the Regional Entities maintain a role in the external review to process to assure that there is sufficient accountability, we leave to the ERO to determine whether the Regional Entities have, or can timely develop, the resources to conduct the external reviews. Alternatively, the ERO may determine that another entity such as reliability coordinators may be best equipped to conduct the reviews. While commenters have made what the Commission believes to be a strong case that reliability coordinators are the appropriate entity to perform the reviews, the ERO should decide the best approach with its understanding of the capabilities and limitations of the Regional Entities. Regardless of this determination, however, the Commission notes that the Regional Entities have the oversight responsibility.

329. Based on the above discussion, the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.

330. The Commission agrees with commenters that critical asset lists contain sensitive information that needs to be protected from public dissemination. The Commission, however, does not believe that this concern is a persuasive rationale for not having an external review mechanism. Rather, adequate safeguards need to be developed to assure that the information contained in critical asset lists are not released during the external review process. While Requirement R4 of CIP-003-1 obligates a responsible entity to "implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets," the Commission does not view this as inherently conflicting with an external review process that has adequate safeguards to prevent the release of sensitive information.

331. In developing an appropriate external review mechanism, the ERO should include features for the controlled delivery of critical assets to the entity performing the external review. Likewise, the ERO should identify minimum safeguards that the external reviewer must deploy to protect sensitive information from disclosure. We agree with commenters' concern that the external reviewer should not become a "central repository" for critical asset lists, and this information should be returned to the responsible entity once the review is complete. The ERO should develop any other safeguards that it believes to be appropriate to protect the disclosure of sensitive information during the external review process.

332. CEA and Manitoba Hydro comment that some Canadian utilities are prohibited from sharing security information with U.S. authorities. They also note that some Canadian utilities regard sharing sensitive security information externally or with a foreign entity as a security risk. In response, the Commission's Final Rule only addresses the obligations of users, owners and operators of the Bulk-Power System in the United States (excluding Hawaii and Alaska). Accordingly, the Commission's directives regarding the development of an external review mechanism applies only to entities subject to the Commission's jurisdiction pursuant to section 215 of the FPA. Whether a similar review process is appropriate or lawful in other jurisdictions is beyond the scope of this Final Rule.

333. Bonneville comments that external review could result in FOIA concerns for Bonneville and other federal entities. It also cautions that external reviewers of critical federal security information may need federal security clearances before being allowed access to classified information. In response to Bonneville, we agree that a governmental entity subject to FOIA requirements should not be required to share sensitive information about critical assets lists that could be deemed a waiver of FOIA protection that is otherwise available. Nonetheless, a governmental entity's identification of critical assets should be subject to appropriate oversight. Thus, we direct the ERO, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information. The ERO should consult with governmental entities that are subject to the CIP Reliability Standards in developing such appropriate provisions and we, likewise, encourage Bonneville and other governmental entities to participate in the development of such provisions.

334. Further, if a governmental entity has classified material regarding its critical assets, this information may not be disclosed except in accordance with controlling laws and regulations. The ERO's external review process must explicitly recognize this limitation.

340. The Commission is sensitive to the concerns raised by the Congressional Representatives regarding the severe impact that a cyber attack on assets not critical to the Bulk-Power System could still have on the public. The Commission, however, believes that its authority under section 215 of the FPA does not extend to other infrastructure. Section 215 of the FPA authorizes the Commission to approve Reliability Standards that "provide for the reliable operation of the bulk-power system," which the statute defines as the facilities and control systems necessary for operation of an interconnected electric energy transmission network and the electric energy needed to maintain transmission system reliability. In addition, section 215(a)(1) specifically excludes from the definition of Bulk-Power System "facilities used in the local distribution of electric energy." Moreover, given the complexities surrounding this issue and the aggressive timeline that will be necessary merely to meet the more modest task of developing and implementing cyber security standards capable of protecting the reliability of the Bulk-Power System, we will follow the approach that we described in the CIP NOPR of approving CIP Reliability Standards designed to safeguard the reliability of the Bulk-Power System.

341. Although the Commission will not direct modifications to the scope of critical assets to be identified under CIP-002-1, for the reasons discussed above, the Commission agrees with commenters regarding the importance of considering interdependencies with other critical infrastructures. The Commission believes that to meaningfully address interdependencies with other critical infrastructures, it is important to coordinate with the stakeholders of these other infrastructures as well as with other government agencies and organizations. Thus, we affirm our CIP NOPR approach that "[w]hile broader interdependency issues cannot be ignored, the Commission intends to revisit this matter through future proceedings and with other agencies. This work will help inform the electric sector and this Commission about the need for future Reliability Standards, especially when the interdependent infrastructures affect generating capabilities, such as through fuel transportation."

344. The commission approves reliability Standard CIP-003-1 as mandatory and enforceable…

355. The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1.

356. In response to ISO/RTO Council, Ontario Power and other commenters, the Commission's intent in the CIP NOPR – as well as the Final Rule – is not to expand the scope of the CIP Reliability Standards. Requirement R1 of CIP-003-1 requires a responsible entity to document and implement a cyber security policy "that represents management's commitment and ability to secure its Critical Cyber Assets." The Requirement then states that the policy, "at a minimum," must address the Requirements in CIP-002-1 through CIP-009-1. The Commission believes that there are other topics, besides those addressed in the Requirements of the CIP Reliability Standards, which are relevant to securing critical cyber assets. The Commission identified examples of such topics in the CIP NOPR. Thus, the Commission, in directing the ERO to develop guidance on additional topics relevant to securing critical cyber assets, is not expanding the scope of the CIP Reliability Standards.

357. Nor do we believe, as suggested by Idaho Power, that the proposed topics for guidance are better addressed by revisions to other Reliability Standards. Again, the guidance is in the context of securing critical cyber assets and is best addressed in the CIP Reliability Standards or a supporting guidance document.

358. In response to SoCal Edison, we disagree that guidance on topics such as power supplies, heating, and other equipment is too detailed for a corporate level policy. These topics are potentially relevant to securing critical cyber assets and, therefore, appropriate topics for guidance.

359. ISO/RTO Council, Ontario Power and other commenters raise concerns regarding potential civil penalty liability if a responsible entity addresses the additional guidance topics in its cyber security policy. The Commission does not believe that the inclusion of additional topics in the cyber security policy will increase a responsible entity's penalty liability. We provide our views regarding the enforcement of cyber security policies below in addressing exceptions to such policies. In particular, we state there that our concern is that a good policy exists and that it is implemented through the exercise of sound reasoning. Consistent with the discussion in the following section, we do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP-003-1) is violated as a result. We do require that the reasoning be documented to ensure that the responsible entity is indeed implementing the security policy as required by Requirement R1 of CIP-003-1.

360. We agree with APPA/LPPC that responsible entities cannot be expected to oversee the operations of commercial communications carriers. However, this is an example of precisely why more guidance would

be useful. Since responsible entities cannot oversee commercial communications carriers, it is important that they consider what they can do to guard against potential threats from that quarter.

372. The Commission continues to believe that it is important that there be ERO and Regional Entity oversight of exceptions from required security policies, however, the Commission agrees with commenters such as EEI and PG&E that this oversight is best accomplished through the existing Regional Entity oversight and audit process.

373. Requirement R1 of CIP-003-1 requires the development and implementation of a security policy. Requirement R3 provides that a responsible entity must document exceptions to its policy with documentation and senior management approval. The Commission is concerned that, if exceptions mount, there would come a point where the exceptions rather than the rule prevail. In such a situation, it is questionable whether the responsible entity is actually implementing a security policy. We therefore believe that the Regional Entities should perform an oversight role in providing accountability of a responsible entity that excepts itself from compliance with the provisions of its cyber security policy. Further, we believe that such oversight would impose a limited additional burden on a responsible entity because Requirement R3 currently requires documentation of exceptions.

374. That being said, the Commission agrees with EEI and others that Regional Entity review of exceptions to a responsible entity's cyber security policy is best accomplished pursuant to the existing Regional Entity audit process where all the relevant facts and circumstances can be considered. Further, review of exceptions to a cyber security policy in the audit process should effectively address commenter concerns regarding disclosure of sensitive information by keeping that data on site.

375. As we discuss elsewhere in the Final Rule, we agree with Bonneville regarding the need to preserve a governmental entity's FOIA protections and address security clearance concerns. The ERO should address these concerns through consultation with relevant governmental entities.

376. Further, the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves.

377. The Requirement to develop and implement a security policy differs from many other Requirements in that it is a means to the end of implementing those Requirements. Our concern that exceptions be documented and justified is primarily a concern that there be reasoned decision-making, consistency, and subsequent effectiveness in implementing the policy. We thus disagree with Northern Indiana that security policy exceptions which do not affect compliance with the Reliability Standards need not be documented. Further, in response to Entergy, as stated elsewhere in this Final Rule, our concern is that a good policy exists and that it is implemented through the exercise of sound reasoning. We do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP-003-1) is violated as a result. We do require that the reasoning be documented to ensure that the responsible entity is indeed implementing the security policy as required by Requirement R1 of CIP-003-1.

378. In response to Northern Indiana's request for clarification of the information that would be required to justify an exception, we leave it to the ERO to provide guidance on the level of information that it considers appropriate, consistent with our discussion above.

381. The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP- 003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The Commission agrees with commenters that the senior manager, by virtue of his or her position, is not a user, owner or operator of the Bulk-Power System that is personally subject to civil penalties pursuant to section 215 of FPA.

386. The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause.

387. In response to Northern Indiana, while we acknowledge that responsible entities are not authorized to enter private homes, we believe that an appropriate cyber security policy will ensure that such information is present in an employee's home only for legitimate reasons specified in the policy and should require the return of all information upon request.

397. Based upon the comments received the Commission is altering its position on how best to address the apparent deficiencies of Requirement R6 in CIP-003-1. The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process.

398. We agree with ISO/RTO Council that the phrase "verification that unintended changes have not been made" captures the core issue. Our concern is that some form of verification is performed to detect when unauthorized changes have been made and to identify those changes, as well as ensuring that the proper alerts are issued.

399. Many of the comments address practical issues involved in addressing accidental consequences and malicious actions, and we recognize that such issues exist. We, thus, agree with Puget Sound that change control and configuration management processes for critical cyber assets cannot ensure 100 percent integrity for those assets when making changes. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. However, we reject Puget Sound's proposal that the Reliability Standard should expressly recognize that absolute assurances are not required. We also believe that our revised directive to the ERO on Requirement R6 addresses Puget Sound's concern about the limitations imposed by a test environment.

400. In response to ReliablityFirst and SPP, we understand that comprehensive regression testing is not necessary for every change regardless of how insignificant. We also agree with ISO/RTO Council that it

can be impractical and unnecessary to verify every intentional automatic change as it occurs. We believe that our revised directive to the ERO addresses these concerns.

407. The Commission proposed in the CIP NOPR that the ERO provide direction, i.e., guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world. The Commission noted that a mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates.

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

409. We agree with Entergy that NIST provides much guidance, but we disagree that it is necessary to define the term mutual distrust. Our proposal is that there be guidance on certain issues and concerns, and we therefore do not believe that a formal definition advances that goal. In response to MidAmerican, we believe that clarification of the terms mutual distrust and outside world, as well as ensuring that any guidelines developed do not harm performance or reliability, are matters that the ERO should consider in the Reliability Standards development process.

410. We disagree with Northern Indiana that Reliability Standards CIP-005-1 and CIP- 007-1 address the matters of concern to us. Northern Indiana does not explain how these Reliability Standards provide guidance of the type we have described. We also disagree that the mutual distrust principle would require responsible entities to sever their communication links with their ISO or RTO or reliability coordinator. The principle could play a role in determining what precautions would need to be taken to protect those communications, but we do not see why it would lead to the specific result that Northern Indiana identifies. Mutual distrust does not imply refusal to communicate; it means the exercise of appropriate skepticism when communicating. The Commission believes additional guidance on what this means specifically in current practice would help responsible entities to avoid these misunderstandings.

411. We disagree with ISO-NE that guidance on mutual distrust is unnecessary because responsible entities either are compliant or they are not, mutual distrust not withstanding. We do not see how responsible entities can fully understand the compliance issues they face without some understanding of how mutual distrust is applied in a modern security environment. Mutual distrust helps explain where an entity's responsibilities begin and end and what assumptions it can make about factors outside its control when it performs its risk-based assessment.

412. The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.
414. …the Commission approves Standard CIP-004-1 as mandatory and enforceable.

431. The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.

432. The Commission notes that commenters did not provide specific reasons why employees should be granted access prior to training, but focused on the nature and scope of our proposed exceptions. Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power System. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.

433. Based on the concerns of commenters, the Commission modifies its CIP NOPR proposal that the ERO identify core training elements to ensure that essential training elements will not go unheeded in emergencies and in other compelling situations. While the Commission continues to believe that the identification of core training elements is useful, this issue would benefit from further vetting within the Reliability Standards development process. Thus, we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard. If the Reliability Standard development process determines not to identify core requirements, the ERO should provide an explanation of this decision. In reply to commenters, we clarify that by using the term core training our concern is for a responsible entity to pre-plan what information and training is necessary for personnel temporarily called in to help in an emergency – not that the actual scope of such training needs to be articulated in the Reliability Standard and applicable to all responsible entities in all circumstances. It is important that responsible entities have plans for introducing the personnel called in to assist in such situations. We expect that core training would be different for different responsible entities.

434. The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets. CIP-004-1 should leave no doubt that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities. We note that, according to Requirement R1.4 of CIP- 005-1, all cyber assets within an electronic security perimeter are to be protected, not just the critical cyber assets. In reply to commenters, we clarify that our proposal discussion on this topic was not intended to suggest that personnel have training that is not appropriate for an employee's duties, functions, experience, or access level. We agree with commenters that information concerning vulnerabilities should be revealed on a need to know basis and not universally. However, any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security.

435. Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves. Commenters provided minimal input on this proposal and, consistent with the CIP NOPR, we believe that whether a modification is appropriate to address this issue is better determined in the first

instance through the ERO's Reliability Standards development process. The ERO should consider the comments of SoCal Edison with regard to what role and steps should be taken by the ERO to ensure quality and consistency of trainers.

443. The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process. FirstEnergy and California Commission agree with the Commission's proposals.

444. ReliabilityFirst and SPP believe that it would be appropriate to handle emergency access via a short-term exception to the security policy. We note that such access would not be only an exception to the security policy, but an exception to a CIP Reliability Standard Requirement. Therefore, such exceptions would have to comply with the conditions of a technical feasibility exception that we have specified elsewhere in this Final Rule. The Commission believes that a workable solution is for the Reliability Standards development process to identify emergency circumstances that would warrant allowing access to critical cyber assets. However, if a responsible entity experienced a situation outside of those circumstances that it believed warranted access to critical cyber assets, the responsible entity could treat the situation as a technical feasibility exception and follow the conditions set out by the Commission. With this approach, we believe that in most cases it will be unnecessary to go through the administrative burden of a technical feasibility exception.

445. SoCal Edison expresses concern that the 30 days allowed in CIP-004-1 for completion of the personnel risk assessment may not be enough time to process all existing employees with access. We note that there is no reason why such assessments cannot be completed well before responsible entities are to be auditably compliant with this provision. The ERO should consider SoCal Edison's issue in the Reliability Standards development process.

446. APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process

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

461. As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate. As noted in the CIP NOPR, most organizations will know in advance the timing of personnel actions and can arrange ahead of time for access revocation to be concurrent with any disciplinary action, transfer, retirement or termination. Revocation of access is usually a matter of assuring that a particular employee's credentials no longer permit physical or electronic access. We understand that outlying elements may require some brief lag before denial of access is effective, in which case, the circumstances justifying such lag must be documented for audit purposes.

462. FirstEnergy comments that the term "immediate" should be clarified and be interpreted as "as soon as possible" but not later than 24 hours to take care of on-the-spot dismissals. Others also comment about various circumstances where advance or coincident preparations for revocation to access cannot be made. We continue to believe that most dismissals can be anticipated in advance and believe that revocation should be immediate upon the employee's notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible.

463. We acknowledge that not all disciplinary actions warrant revocation of access privileges. In addition, certain personnel transfers can require a protracted transitional process that warrants retention of access privileges after the formal transfer date. There may be operational reasons that justify retention of access privileges after an employee transfers, but the default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes.

464. We also adopt our proposal to default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes. Our concern, in calling for this adjustment, is that the current language in the CIP Reliability Standard does not describe the purpose of the required list of personnel with authorized access; rather, it merely states that such a list must be made, reviewed, and updated. Similar to our expectations expressed earlier regarding implementation of required plans and policies, we believe that the expectation that access not be granted to personnel not on the authorized list should be made clear in the Reliability Standard. However, while a responsible entity should not allow access to any personnel not included on the list, the Commission believes commenters misunderstood the CIP NOPR and inappropriately linked the Commission's proposal with respect to the immediate revocation of access with its proposal with respect to denying access to personnel not on the list. We clarify that we are not requiring the list to be updated simultaneously with the revocation of an employee's access.

473. The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.

474. Regarding Northern Indiana's comments, we do not believe that this Requirement obligates one joint owner of a critical cyber asset to perform risk assessments of another owner's personnel. Each such owner is responsible for performing assessments of its own personnel.

475. The ERO should consider the suggestions raised by Northern Indiana, SPP and NRECA in the Reliability Standards development process. 476. Therefore, we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commission's determinations above.

478. The Commission approves Standard CIP-005-1 as mandatory and enforceable.

496. The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter. However, in light of the comments received, the Commission understands that there may be instances in which certain

facilities cannot implement defense in depth or where such an approach would harm reliability rather than enhance it. For that reason, the Commission believes that it is appropriate to allow the ERO and the Regional Entities to grant exceptions based on the technical feasibility of implementing defense in depth, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement electronic defense in depth measures or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

497. As stated in the CIP NOPR, the Commission recognizes that there is a point at which having multiple defense layers would not be cost effective. However, we continue to believe that the effectiveness of any one defense measure is often dependent on the quality of active human maintenance, and there is no one perfect defense measure that will guarantee the protection of the Bulk-Power System. The Commission does not agree with Manitoba that providing one monitored and alarmed electronic security measure provides a sufficient and balanced security measure when implemented in conjunction with required physical security measures. A single electronic device is too easy to bypass and a physical security measure cannot thwart an electronic cyber attack. Therefore, we believe it is in the public interest to require that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter.

498. Many of the commenters' concerns with regard to the impact on performance and reliability will be alleviated by allowing Regional Entities to grant justified exceptions based on technical feasibility. For example, an exception might be granted if an entity can demonstrate that implementing any defense in depth mechanism would create a delay in the transmission of the data that is not tolerable on the system and cannot be mitigated. In addition, the Commission does not think that there will be a problem with respect to a delay in data transmission. If this is a problem for older or distant equipment, the responsible entity can claim a technical feasibility exception. Newer equipment should operate at sufficiently high speeds that multiple hops will not affect data transmission. In fact, some vendor companies claim that their devices will actually increase transmission speeds due to compression and other techniques.

499. Further, an exception might be granted until equipment is available for a given protocol or toolset used in a specific control system environment. However, the fact that additional equipment may take up space or use additional power and cooling alone does not warrant reversing the Commission proposal.

500. The Commission agrees with the ERO that requiring two or more defensive measures may increase the chance of equipment failure. But, the ERO has not provided the Commission with an adequate explanation of why the availability of the entire system would decrease with two or more defensive measures. Defensive measures can often be formatted so that if they fail, they do so in a fail-safe mode that still allows operation. Therefore, system availability would not decrease.

501. In response to SDG&E and Entergy, in stating that the placement of security measures in front of systems provides a layer of protection for those systems, the Commission was not giving priority to "in front" measures. In fact, the Commission acknowledged in the CIP NOPR that defense in depth measures are generally integrated within and constitute part of a system or program. In commenting that defense in depth measures may also be effectively placed in front of a system, the Commission intended only to acknowledge that there are multiple ways to implement a defense in depth strategy. The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity have at least two security measures unless it is not technically feasible to do so. The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment. The Commission believes that this, in conjunction with the allowance of technical feasibility exceptions, alleviates FPL Group's concern that the Commission's proposal is a "one size fits all" approach.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process. This would include whether or not the second security measure must be "on par" with the first. The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

503. In response to Manitoba's concern that the proposed additional security measure could delay implementation of the more important requirement of an electronic perimeter for all critical cyber assets, the Commission notes that this Final Rule approves the Reliability Standard as filed by the ERO. The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures. Until that Reliability Standard is developed by the ERO and approved by the Commission, responsible entities in the United States will not be required to implement two or more defensive measures.

504. The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device."

511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document.

525. The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily, as requested by Juniper.

526. The Commission agrees with MidAmerican that the review intervals should be designed to accomplish the detection and improvement objectives discussed in the CIP NOPR. Requirement R3 of CIP-005-1 does not currently require a responsible entity to manually review logs if it has alerts. However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches,

periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Further, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs. The Commission believes allowing 90 days to pass without a log review is unacceptable. In that time, an incident could have occurred undetected or an attacker could have gained access to a critical system and extended that access throughout the enterprise with the targeted entity being unaware that the security of their systems had been compromised. For this reason, the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments. The Commission continues to believe that, in general, logs should be reviewed at least weekly, but leaves it to the Reliability Standards development process to determine the appropriate frequency. In addition, the Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.

527. In response to MidAmerican's concern about the term "bifurcated review," the Commission intent was that certain assets, deemed readily accessible, would be reviewed at least weekly while other assets would continue to be reviewed every 90 days. However, the Commission will not adopt this direction from the CIP NOPR. We leave it to the Reliability Standards development process to decide whether different timeframes are appropriate for logs that are readily accessible and not readily accessible. If different review timeframes are adopted, the ERO should provide guidance as to what constitutes a readily accessible log and a log that is not readily accessible. The ERO may also delineate different timeframes for manual review for other reasons, but must clearly define how to determine in what timeframe a specific log must be reviewed. However, we reiterate that any attempt to differentiate the required frequency of review of these logs must be balanced against the criticality of the facilities; it is not acceptable to dismiss a critical facility from timely review simply because it is remote.

528. Finally, the Commission also agrees with commenters that a full review of logs could be burdensome. Therefore, the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that the manner in which a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, any requirements for creating this sample review could be detailed in its cyber security policy so that it can be audited. The Reliability Standards development process should decide the degree to which the revised CIP-005-1 describes acceptable log sampling. The ERO could also provide additional guidance on creating the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the responsible entity to detect intrusions by attackers.

541. The Commission notes that the concerns expressed by some commenters of triggering an unknown vulnerability during a live test is one reason why some form of live or active testing is necessary. A responsible entity cannot protect its system from exploitation of vulnerabilities that it does not know about. However, in light of the comments received, the Commission will not adopt its proposal as set out in the CIP NOPR regarding live vulnerability assessments in Requirement R4 of CIP-005-1. Instead, we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments. Further, as discussed below, we clarify that an interim vulnerability assessment will only

need to be performed if a responsible entity makes a significant modification to the electronic security perimeter.

542. The Commission's goal in proposing live vulnerability testing is to provide a level of confidence that the Bulk-Power System has a certain level of resistance to attack. We understand the concerns raised by commenters that live vulnerability testing could, at this time, diminish reliability. While the Commission's goal is to require full live vulnerability testing on the entire Bulk-Power System at some point, we understand that this may not be possible at this time. As suggested by FirstEnergy, industry may need time to gain experience in this area before it can conduct full live vulnerability testing. Therefore, the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.

543. The Commission agrees with the ERO that test systems do not need to exactly match or mirror the operational system. However, to perform active vulnerability assessments, the responsible entities should be required to create a representative system, i.e., one that replicates the actual system as closely as possible. The active vulnerability assessment should be carried out on this representative system. In doing so, a responsible entity must document the differences between the operational and representative system for the auditors. As part of this documentation, the responsible entity should also document how test results on the representative system might differ from the operational system, and how the responsible entity accounts for such differences in operating the system. Our goal is to ensure that each responsible entity understands the differences between its representative system and the operational system and how those differences might affect its test results. The entities remain responsible, however, to ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.

544. Further, the Commission agrees with commenters that requiring each responsible entity to perform a vulnerability assessment of the electronic access points when any modification is made to the electronic security perimeter or defense in depth strategy is too broad. Instead, the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification. To be clear, the Commission is not requiring the Reliability Standard to use the terminology that a "significant change" is made to the electronic security perimeter or defense in depth strategy. Rather, we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment. For example, we would anticipate that updating an attack signature file on the electronic access point would not require an active vulnerability assessment, but replacing the devices that comprise the electronic access point would require an active vulnerability assessment.

545. Given our changes to the Commission proposal, and based upon the comments, the Commission does not believe performing an active vulnerability assessment once every three years will pose too great a burden on company personnel. The burden above that is required by the Reliability Standard as proposed by the ERO is justified by the insights that will be gained from the active assessments.

546. At this time, the Commission does not believe it is necessary to require twice a year penetration tests by responsible entities, as requested by Juniper. We believe that the combination of annual testing and active vulnerability assessments is sufficient for the Reliable Operation of the Bulk-Power System.

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a

representative system and what modifications require an active vulnerability assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

559. We are persuaded by commenters that there may be instances in which the physical or safety-related obstacles to achieving a completely enclosed physical boundary cannot be overcome. In such instances, we agree with commenters that it would be inappropriate to treat the alternative measures under this CIP Reliability Standard as interim actions under the technical feasibility exception, as the exception was proposed in the CIP NOPR. However, the Commission has revised its determination with respect to the technical feasibility exception to address concerns such as those raised by commenters on Requirement R1.1 of CIP-006-1. The Commission believes that allowing a technical feasibility exception to Requirement R1.1 of CIP-006-1, with the changes discussed in the Technical Feasibility section of this Final Rule, should address commenters' concerns. Specifically, the Commission acknowledges that some circumstances merit reliance on mitigation strategies that are ongoing and effective, so long as they are justified and reviewed periodically. This should alleviate the concern of commenters that the Commission is not allowing exceptions to Requirement R1.1 on a long-term basis.

560. Therefore, the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions. In evaluating the requests for a technical feasibility exception to Requirement R1.1, we expect the ERO to work with the responsible entities to ensure consideration of any emerging technologies that may allow the responsible entity to satisfy Requirement R1.1.

572. The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets. However, similar to our determination in CIP-005-1 regarding defense in depth for electronic security perimeters, in light of the comments received, the Commission understands that there may be instances in which certain facilities cannot implement defense in depth or where such an approach would harm reliability rather than enhance it. For that reason, the Commission believes that it is appropriate to allow the ERO and the Regional Entities to grant exceptions based on the technical feasibility of implementing defense in depth, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement physical security perimeter defense in depth measures or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

573. As stated in the CIP NOPR, the Commission recognizes that there is a point at which implementing multiple layers of defense becomes an unreasonable burden to responsible entities. However, as more fully detailed in our discussion of defense in depth in CIP-005-1, we continue to believe that the effectiveness of any one defense measure is often dependent on the quality of active human maintenance, and there is no one perfect defense measure that will guarantee the protection of the Bulk-Power System. Therefore, we continue to require the use of layered and complementary security procedures that a defense in depth approach embodies.

574. In response to APPA/LPPC's comments, the Commission does not require two or more different monitoring methods under Requirement R3. We did not propose to modify Requirement R3 and are not doing so in this Final Rule. Further, the Commission did not intend to require two or more physical perimeters, as suggested by NERC and ReliabilityFirst. Rather, the Commission intended only to require

the ERO to modify R2 to provide for two or more different and complementary physical assess controls at a physical access point of the perimeter. The Commission believes that this should clarify what it meant by the term "procedures" and sees no need to direct the ERO to define the term, as requested by Entergy.

575. In response to commenters' questions regarding specific physical access controls, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant physical security. While the Commission continues to believe that a responsible entity must implement two or more distinct and complimentary physical access controls at a physical access point of the perimeter, the specific requirements should be developed in the Reliability Standards development process when the ERO develops its modifications in response to this Final Rule. The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

576. Northern Indiana raises a concern about security measures in remote or field locations, but did not provide specific information. The Commission believes that, if it is not possible to implement two or more distinct physical security measures in a remote or field location, a Regional Entity could grant justified exceptions based on technical feasibility.

581. The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years, but clarifies our direction in several respects. Similar to our action with respect to reviewing logs in CIP- 005-1, the Commission will not adopt the proposal to require different testing periods for physical security measures on critical cyber assets that are readily accessible or not readily accessible. Instead, we leave it to the Reliability Standards development process to decide whether different timeframes are appropriate for physical security measures on critical cyber assets that are readily accessible and not readily accessible. Similar to our direction in CIP-005-1, if different review timeframes are adopted, the ERO should provide guidance as to what constitutes a readily accessible facility and a facility that is not readily accessible. The ERO may also delineate different timeframes for testing for other reasons, but must clearly define how to determine in what timeframe the physical security measures on a specific critical cyber asset must be reviewed.

582. In response to Northern Indiana, the Commission does not believe it is necessary at this time to specify what would constitute a test, because each test may be different based on the type of physical security measure employed. Northern Indiana may ask the ERO to provide guidance on this matter.

583. In response to National Grid, we clarify that the CIP NOPR's reference to the testing of critical cyber was inadvertent, and that we proposed testing intervals for physical security measures.

585. The Commission approves Reliability Standard CIP-007-1 as mandatory and enforceable.

597. The Commission affirms its proposals with respect to technical feasibility and acceptance of risk. Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2. However, as discussed in the CIP NOPR, this leaves intact the exception for technical limitations in Requirement R2.3, so long as the treatment of Requirement R2.3 conforms to our findings regarding the technical feasibility exceptions.

598. MidAmerican's concerns about clarifying the terms technical limitations and technical feasibility through the Reliability Standards development process are addressed in our findings regarding technical feasibility elsewhere in the Final Rule.

599. In response to Juniper, the Commission does not believe that applying the technical feasibility exception in lieu of acceptance of risk means that a responsible entity would not have to mitigate the risk of not being able to turn off ports. The Commission believes that our discussion of the technical feasibility exception in the Technical Feasibility Exception Remediation and Mitigation section above supplies the obligation to mitigate that Juniper is seeking.

600. With respect to security patch management, the Commission continues to believe that the acceptance of risk language is unacceptable. However, in doing so we do not seek to prevent responsible entities from exercising some level of discretion. The Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility. The Commission believes that this will allow responsible entities the discretion APPA/LPPC seek. Further, this essentially accomplishes the outcome sought by MidAmerican. With respect to the disclaimer requested by APPA/LPPC, the Commission is not convinced to direct such a modification to the Reliability Standard at this time. However, this issue should be examined in the Reliability Standards development process. Given that we are modifying our direction, we do not believe that it is necessary to mandate senior management involvement in these decisions here. While we direct the ERO to modify Requirement R3 of CIP-007-1 to remove the acceptance of risk language, the ERO, through the Reliability Standards development process may choose to allow exceptions to this requirement for technical infeasibility, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement the requirements for software patches for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

609. The Commission has discussed issues related to testing environments in CIP-005- 1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a "representative system" – one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.

610. Consistent with our action in CIP-005-1, the Commission will not at this time require documentation of each difference between the testing and the production environments and how each such difference is mitigated or otherwise addressed. In using the term mitigation, our goal was to ensure that each responsible entity understands the differences between its representative system and the production system and how those differences might affect its test results. The Commission believes that, as a part of this documentation, the responsible entity should also document how any test results might differ from the testing system to the production system and how the responsible entity accounts for such differences in operating the system. Therefore, we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above. Such revision should address what types of differences must be documented. The entities remain responsible, however, to ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.

611. With respect to MidAmerican's proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO

should consider this matter in the Reliability Standards development process. However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.

612. The Commission understands Northern Indiana's concern that documenting vulnerability test results or any mitigation or remediation plans may reveal system vulnerabilities. The ERO should alleviate this concern by providing for such reports to be reviewed under the confidentiality provisions of its Rules of Procedure.

619. The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. Issues concerning technical feasibility and acceptance of risk are discussed above.

620. The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used. Further, as Consumers admits, any network infrastructure devices that are not directly targeted can be affected as collateral damage.

621. While we agree that no safeguard will protect against all malicious or unintentional acts, this does not mean that systems should not be protected against such acts. In response to MidAmerican, the Commission believes that details regarding how to safeguard systems against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset are best developed in the Reliability Standards development process. The revised Reliability Standard does not need to prescribe a single method for protecting against the introduction of viruses or malicious software to a cyber asset by personnel. However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance with the Reliability Standard. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes how an entity should protect against personnel introducing viruses or malicious software to a cyber asset. The ERO could also provide additional guidance in a reference document.

622. Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

628. Requirement R6 of CIP-007-1 does not address the frequency with which logs should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP- 007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1. Also, at this time, the Commission

does not believe that it is necessary to require responsible entities to maintain all logs for at least three years, as requested by Juniper.

629. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

630. In response to Northern Indiana, the Commission discusses our use of the term forensics in our discussion of CIP-009-1.

633. The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. The Commission notes that there is a difference between redeploying an asset and discarding it. Redeploying an asset within the same responsible entity allows that responsible entity to maintain control over the asset, whereas disposing of an asset places it out of the control of the responsible entity. The Commission believes that, while the seven layer wipe described by Northern Indiana may be sufficient for redeployment because the responsible entity maintains control over the cyber asset, it is not sufficient for disposing of an asset.

634. The Commission disagrees with Northern Indiana that the only way to allow no opportunity to access data on storage media is to destroy the media. As stated in the CIP NOPR, high quality degaussing can adequately protect media from unauthorized access. [SRM1]Northern Indiana has not provided information that convinces the Commission that a cyber asset would have to be destroyed in order to prevent access.

635. Therefore, the Commission directs the ERO to revise Requirement R7 of CIP-007- 1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.

643. The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.

644. The Commission agrees with ISO-NE that hardware and software is implemented in diverse ways throughout the industry, but does not believe that this renders providing guidance infeasible. We also agree that overly rigid guidance could result in responsible entities failing to properly test for vulnerabilities specific to the entities' environments and systems. The Commission does not believe that the revised Reliability Standard should be inflexible. It should encourage responsible entities to take into account emerging and diverse technologies and newly discovered vulnerabilities as they emerge. The Commission believes that it is appropriate to leave such guidance to the Reliability Standards development process. Further, we leave it to the ERO's discretion whether to put guidance in the revised Reliability Standard or a reference document.

645. The Commission addressed Northern Indiana's concerns about revealing vulnerability test results in our discussion of CIP-005-1. We believe that the ERO's confidentiality provisions should adequately protect against unwanted disclosure of vulnerability test results.

651. The Commission adopts a modified version of the CIP NOPR proposal. We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days. The Commission believes that 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation.

652. The Commission clarifies that the shorter period should begin upon final implementation of the modifications. The Commission believes that providing that the shorter period begins when the modifications are implemented satisfies Northern Indiana's concern about finalizing documentation and the potential need for internal reviews and approvals. By the time any modification is made, such approvals should already have been granted. Similarly, the Commission believes that MidAmerican's concern about resource constraints relate more to the implementation of a modification, not the documentation of that implementation. Once a modification is developed and implemented, documenting it should not consume significant time or resources.

660. The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident.

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

673. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. As stated in the CIP NOPR, the reporting timeframe should run from the discovery of the incident by the responsible entity, and not the occurrence of the incident.

674. Most commenters are concerned with the burden placed on a responsible entity to report an incident when system restoration should take precedence. As stated in the CIP NOPR, while the Commission

agrees that, in the aftermath of a cyber attack, restoring the system is the utmost priority, we do not believe that sending this short report would be a time consuming distraction, and we judge that its probative value would justify the minimal time spent in making this report. In this respect, the Commission now clarifies that the responsible entity does not need to initially send a full report of the incident. Rather, to report to appropriate government authorities and industry participants within one hour, it would be sufficient to simply communicate a preliminary report, including the time and nature of the incident and whatever useful preliminary information is available at the time. This could be accomplished by a phone call or another method. The responsible entity could then follow up with a full report once the system is restored.

675. With respect to the arguments by California Commission and Texas PUC concerning the term appropriate government authorities, we believe this determination should be made through the Reliability Standards development process.

676. Thus, the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. The Reliability Standard development process should consider whether the ESISAC could act as an intermediary to promptly notify government authorities for responsible entities. While we expect the modified Reliability Standard to be consistent with our discussion above, we leave development of the details of how to report incidents while not burdening the recovery process to the Reliability Standards development process.

677. With respect to Entergy's question about the relationship between CIP-001-1 and CIP-008-1, the ERO should consider Entergy's concerns in the Reliability Standards development process. However, the Commission notes that, while CIP-001-1 requires the reporting of sabotage events, CIP-008-1 requires the reporting of all cyber security incidents. Not all cyber security incidents will be caused by sabotage, so not all incidents required to be reported under CIP-008-1 will be required to be reported under CIP-001-1.

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

687. In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise.

689. The Commission approves Reliability Standard CIP-009-1 as mandatory and enforceable.

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

706. The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard. The Commission continues to believe that it is important to long-term reliability interests that responsible entities collect data in certain situations, such as immediately after system restoration or the recovery of critical cyber assets. In response to ISO-NE, the Commission does not believe that the requirement to keep log data contained in other CIP Reliability Standards is sufficient. As we stated in the CIP NOPR, the data collection procedures could include preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data. None of this is required in the Reliability Standards cited by ISO-NE.

707. The Commission used the term forensic because that is the term used in the Blackout Report. However, the Commission clarifies that it does not intend, as suggested by commenters, that the Reliability Standard impose the extent of scientific rigor or chain of custody required in criminal procedure. Rather, the Commission is concerned with responsible entities preserving the data necessary to determine the cause of any problem with the system.

708. In response to Entergy, NRECA, SoCal Edison and Northern Indiana, recovery of critical cyber assets and the Bulk-Power System is of immediate critical importance, and information collection efforts should not impede or restrict system restoration, as stated in the CIP NOPR. We agree that preserving evidence should not hinder system restoration.

709. We do not object to the alternate proposal developed by the ERO, including use of the phrase "data collection for post-event analysis, where technically feasible," to describe what should be required under the revised Reliability Standard. The ERO may also consider the methods proposed by Entergy and MidAmerican. We also recognize that collecting forensic data may not be technically feasible for all situations due to equipment limitations, such as older substation installations with little electronic monitoring. Therefore, when revising the Reliability Standard, the ERO may incorporate a technical feasibility exception, subject to the same conditions for exercising the exception as described elsewhere in this Final Rule.

710. Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report. The modification should focus on responsible entities preserving the data necessary to determine the cause of any problem with the system and may include a technical feasibility exception.

725. The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years. Consistent with our goals and discussion of CIP-005-1, the Commission will not at this time require responsible entities to perform full operational exercises. Instead, the Reliability Standard should require the demonstrated recovery of critical cyber assets in a test environment, with the requirements for representative test environments and for addressing differences between the test environment and the production environment, similar to the conditions discussed for live

testing in CIP-005-1. Given the range of views presented in comments regarding live testing, as the Reliability Standard development process forms the details of this "demonstrated recovery" concept, it should consider offering guidance beyond the actual Requirements of the Reliability Standard in separate reference documents. The Commission believes this alleviates commenters' concerns about the risks associated with such testing

726. The Commission notes ISO-NE's concerns about providing a definition of full operational exercise in the NERC Glossary are addressed since we are not requiring the use of that term in the Reliability Standards.

731. The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans. We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective. As we stated with respect to change made pursuant to CIP-007-1, the Commission believes that having correct documentation is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could attempt to operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation. Northern Indiana has not provided us sufficient reason to change the CIP NOPR proposal. Finally, as stated with respect to the documentation requirements in CIP-007-1, the 30 day period should begin upon final implementation of the modifications.

739. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes. Our intent in doing so is to require responsible entities to have a procedure in place that gives them a high confidence level that their backups will actually restore the system as needed. Auditors should be able to determine compliance by reviewing a responsible entity's policies, procedures and records to determine how the testing is done and what recent tests have been performed. In response to commenters' suggestions on how to verify the backup and restoration processes, the ERO should determine appropriate methods to accomplish the Commission's objectives in the Reliability Standards development process.

740. The Commission does not agree with FirstEnergy and Northern Indiana that requiring verification of backup and restoration processes and procedures when a significant change is made to the operational control system requires continuous assessment. The Commission does not believe that every change will necessitate verification of the backup and restoration processes. Rather, it is sufficient to verify a process if a significant change, such as adding new hardware or installing new software to the control system, is made. The Commission does not believe that responsible entities will be making significant changes to their backup and restoration processes continuously. Similar to our determination with respect to Requirement R4 of CIP-005- 1, the ERO should determine, through the Reliability Standards development process, what would constitute a modification that would require verification of the backup and restoration processes.

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

Commission agrees with ISO-NE that it is impractical to require the system to be shut down and be restarted with the data in order to test it. As stated above with respect to verifying backups after a significant change, our intent is to give responsible entities a high confidence level that their backups will actually restore the system as needed. Auditors should be able to look at a responsible entity's policies, procedures and records to determine how the testing is done and what recent tests have been performed. The ERO should determine appropriate methods to accomplish the Commission's objectives in the Reliability Standards development process.

757. NERC and other commenters ask the Commission to defer to NERC on the determination of Violation Risk Factors and allow NERC to reconsider the designations using the Reliability Standards development process. The Commission has previously determined that Violation Risk Factors are not a part of the Reliability Standards. In developing its Violation Risk Factor filing, NERC has had an opportunity to fully vet the CIP Violation Risk Factors through the Reliability Standards development process. The Commission believes that, for those Violation Risk Factors that do not comport with the Commission's previously-articulated guidelines for analyzing Violation Risk Factor designations, there is little benefit in once again allowing the Reliability Standards development process to reconsider a designation based on the Commission's concerns. Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations. NERC must submit a compliance filing with the revised Violation Risk Factors no later than 90 days before the date the relevant Reliability Standard becomes enforceable.

758. That being said, NERC may choose the procedural vehicle to change the Violation Risk Factors consistent with the Commission's directives. NERC may use the Reliability Standards development process, so long as it meets Commission-imposed deadlines. In this instance, the Commission sees no vital reason to direct the ERO to use section 1403 of its Rules of Procedure to revise the Violation Risk Factors below, so long as the revised Violation Risk Factors address the Commission's concerns and are filed no less than 90 days before the effective date of the relevant Reliability Standard. The Commission also notes that NERC should file Violation Severity Levels before the auditably compliant stage.

759. Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.

760. The Commission disagrees with Progress that the Commission's concerns with respect to the CIP Violation Risk Factors will result in overly conservative Violation Risk Factor assignments. We also disagree with the characterization that a Violation Risk Factor delineates the importance of the Reliability Standard. Rather, the Violation Risk Factors delineate the relative risk to the Bulk-Power System associated with the violation of each Requirement. The Commission believes that the analysis below appropriately takes into account the risk of violating each Requirement in the CIP Reliability Standards.

767. The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors. While the Commission hopes that APPA/LPPC are correct that there is not a substantial potential for assets to be overlooked, this is not a reason to not modify the Violation Risk Factors. As we stated in Order No. 672, the fundamental goal of mandatory, enforceable Reliability Standards and related enforcement programs is to promote behavior that supports and improves Bulk-Power System reliability. It is not imposing penalties. However, as APPA/LPPC recognize, overlooked assets could result in Bulk-Power System failure. This comports with the definition of a high Violation Risk Factor as a requirement that, if violated, could directly cause or contribute to Bulk-Power System instability, separation, or a cascading sequence of failures, or could place the Bulk-Power System at an unacceptable risk of

instability, separation, or cascading failures. APPA/LPPC have not provided a persuasive reason for the Commission to change its proposal to direct the ERO to modify the Violation Risk Factors.

768. Further, the Commission is not persuaded by the argument that the Violation Risk Factor should not be high because there is an incentive for responsible entities to proceed cautiously. The Violation Risk Factor should consider the risk to the system of noncompliance, regardless of other incentives that users, owners and operators of the Bulk- Power System have to comply.

769. Finally, the regional oversight over asset designation discussed by APPA/LPPC is not in place yet. Therefore, the Commission cannot rule on what it might be.

776. MidAmerican seems to misunderstand the purpose of the information collection statement. The OMB regulations require agencies to submit a burden estimate for collections of information contained in proposed rules, not for the entire cost of compliance. As stated in the CIP NOPR, the Commission only included the cost of developing the required documentation for the required policies, plans, programs and procedures in its burden estimate, but did not include in our burden estimate the cost of substantive compliance with the CIP Reliability Standards. MidAmerican raises concerns regarding the total cost of compliance with the Reliability Standards, rather than the burden associated with reporting requirements in the Reliability Standards. Therefore, the Commission does not believe it is necessary to revise the burden estimate based on MidAmerican's comments.

799. As of October 2007, there are 1,772 registered entities, of which the Commission estimates that approximately 1,400 will be responsible for compliance with the CIP Reliability Standards. Of these, the Commission estimates that the CIP Reliability Standards would apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipal and cooperatives.

800. Arkansas Electric raises concerns with the cost to small entities of the modifications directed by the Commission. These modifications will be made by the ERO through the Reliability Standards development process. Until NERC files any revised Reliability Standards, the Commission cannot estimate their burden on any user, owner or operator of the Bulk-Power System, including small entities. The Commission therefore does not believe it is appropriate to speculate on the cost of compliance with any modified Reliability Standard at this time.

801. The Commission does not believe it is appropriate to grant California Cogeneration's request that NERC develop pro forma models of protocols and methodologies to be used by entities to facilitate compliance. As discussed in the section regarding guidance, that level of detail could potentially introduce common vulnerabilities resulting from all small entities implementing the Reliability Standards using a nearly identical solution. With respect to California Cogeneration's suggestion that NERC should have a formal role in collaborating to reduce compliance costs, the Commission will not direct that at this time. However, NERC should consider providing information to such groups. Further, the Commission believes that requiring the ERO to develop guidance on how to comply with the Reliability Standards should facilitate compliance by small entities.

802. The Commission also declines to direct the ERO to include a QF category in the Functional Model, as requested by Energy Producers. The Commission believes that this request is outside the scope of this rulemaking, which only concerns the CIP Reliability Standards proposed by NERC.

803. The Commission does not believe it is necessary to allow small entities a longer compliance timetable or to provide temporary waivers upon an adequate showing of work to attain compliance. As we stated in the CIP NOPR, the burden to small entities is not great, but the economic impact is justified as

necessary to protect cyber security assets that support Bulk-Power System reliability. Further, the Commission believes that allowing small entities to collectively select a single consultant to develop model software and programs to comply with the CIP Reliability Standard will allow the small entities to take advantage of any information known by larger entities or their consultants.

804. While Southwest TDUs are correct that the Commission acknowledges that the Reliability Standards could be made applicable down to the smallest entity, the Commission disagrees that this discounts the economic impact on these entities. As we stated in the CIP NOPR, to be included in the compliance registry, the ERO will have made a determination that a specific small entity has a material impact on the Bulk-Power System. A small entity placed on the compliance registry could then appeal the determination to the ERO and the Commission.

805. Further, Southwest TDUs argue that just because a larger entity is performing compliance does not mean the costs of compliance are not being passed on to the small entities. We agree; however, in allowing small entities to pool their resources and select a single consultant to develop model software and programs, each entity need not separately fund model software and programs development. Rather, that cost can be spread over several entities.

806. For the reasons stated in the CIP NOPR and above, the Commission certifies that this rule will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-1

3. Purpose: NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

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

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:

M1. The risk-based assessment methodology documentation as specified in Requirement R1.

M2. The list of Critical Assets as specified in Requirement R2.

M3. The list of Critical Cyber Assets as specified in Requirement R3.

M4. The records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002 from the previous full calendar year

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1 Level 1: The risk assessment has not been performed annually.

2.2 Level 2: The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.

2.3 Level 3: The list of Critical Assets or Critical Cyber Assets does not exist.

2.4 Level 4: The lists of Critical Assets and Critical Cyber Assets do not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change “Control Center” to “control center”	03/24/06

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-1

3. Purpose: Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-003, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-003:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

R2.1. The senior manager shall be identified by name, title, business phone, business address, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

M1. Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.

M3. Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.

M4. Documentation of the Responsible Entity's information protection program as specified in Requirement R4.

M5. The access control documentation as specified in Requirement R5.

M6. The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,

2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,

2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,

2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,

2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

2.4.1 No cyber security policy exists; or,

2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,

2.4.3 No documented change control and configuration management process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-1

3. Purpose: Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-004, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-004:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-004:

R1. Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

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

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:

M1. Documentation of the Responsible Entity's security awareness and reinforcement program as specified in Requirement R1.

M2. Documentation of the Responsible Entity's cyber security training program, review, and records as specified in Requirement R2.

M3. Documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. Documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.3.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,

2.1.2 Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,

2.1.3 Personnel risk assessment program exists, but documentation of that program does not exist; or,

2.1.4 List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.

2.1.5 One personnel risk assessment is not updated at least every seven years, or for cause; or,

2.1.6 One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.

2.2. Level 2:

2.2.1 Awareness program does not exist or is not implemented; or,

2.2.2 Training program exists, but does not address the requirements identified in Standard CIP-004; or,

2.2.3 Personnel risk assessment program exists, but assessments are not conducted as required; or,

2.2.4 One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.

2.3. Level 3:

2.3.1 Training program exists, but has not been reviewed and updated at least annually; or,

2.3.2 A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,

2.3.3 List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.

2.4. Level 4:

2.4.1 No documented training program exists; or,

2.4.2 No documented personnel risk assessment program exists; or,

2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel termination for cause…”	03/24/06
1	06/01/06	D.2.1.4 — Change “access control rights” to “access rights.”	06/05/06

A. Introduction

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

2. Number: CIP-005-1

3. Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability

4.1. Within the text of Standard CIP-005, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-005:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; and,

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

M1. Documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's annual vulnerability assessment as specified in Requirement R4.

M5. Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,

2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,

2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-1

3. Purpose: Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-006, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-006:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

R2. Physical Access Controls **—** The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms

for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

R5. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:

R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.

R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the review and updating of the plan.

M2. Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.

M3. Documentation identifying the methods for monitoring physical access as specified in Requirement R3.

M4. Documentation identifying the methods for logging physical access as specified in Requirement R4.

M5. Access logs as specified in Requirement R5.

M6. Documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documents other than those specified in Requirements R5 and R6.2 from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,

2.1.2 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.1.3 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

2.1.4 Physical access logs are retained for a period shorter than ninety days; or,

2.1.5 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

2.1.6 One required document does not exist.

2.2. Level 2:

2.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

2.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

2.2.4 More than one required document does not exist.

2.3. Level 3:

2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,

2.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

2.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.4.3 No maintenance or testing program exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-1

3. Purpose: Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-007, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-007:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

M1. Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.

M2. Documentation as specified in Requirement R2.

M3. Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.

M4. Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.

M5. Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.

M6. Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.

M7. Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. Documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or

2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,

2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
- Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

2.2. Level 2:

2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,

2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.3. Level 3:

2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,

2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4. Level 4:

2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,

2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4.3 No logs exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-1

3. Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability

4.1. Within the text of Standard CIP-008, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-008:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-008:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all

reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of CIP-008:

M1. The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan

M2. All documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.4.4 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Levels of Noncompliance

2.1. Level 1: A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.

2.2. Level 2:

2.2.1 A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,

2.2.2 A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,

2.2.3 Records related to reportable Cyber Security Incidents were not retained for three calendar years.

2.3. Level 3:

2.3.1 A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,

2.3.2 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.

2.4. Level 4: A Cyber Security Incident response plan does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-1

3. Purpose: Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability:

4.1. Within the text of Standard CIP-009, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Reliability Organizations

4.2. The following are exempt from Standard CIP-009:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-009:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:

M1. Recovery plan(s) as specified in Requirement R1.

M2. Records documenting required exercises as specified in Requirement R2.

M3. Documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. Documentation regarding backup and storage of information as specified in Requirement R4.

M5. Documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-009 from the previous full calendar year.

1.3.2 The Compliance Monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,

2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.

2.2. Level 2:

2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,

2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.

2.3. Level 3:

2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,

2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.

2.4. Level 4:

2.4.1 No recovery plan(s) exist; or,

2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 7, 2008

TO: NERC BOARD OF TRUSTEES
NERC STAKEHOLDERS

Ladies and Gentlemen,

NERC has recently come under scrutiny with respect to our response to certain specific cyber security vulnerabilities identified by the Department of Homeland Security (Aurora) as well as the effectiveness of our overall critical infrastructure protection program. It is absolutely essential that NERC responds swiftly and effectively to such criticisms and that the industry continues to address cyber vulnerabilities that could impact the reliability of the bulk power system (BPS).

NERC, as the international electric reliability organization (ERO), must be at the forefront with respect to cyber security. NERC needs to do a better job of communicating industry efforts to mitigate threats to cyber security and must do more, in a coordinated manner, to help policy makers address the critical infrastructure protection concerns faced by the industry.

NERC and the industry share a mutual goal to ensure that threats to the reliability of the BPS, especially cyber security threats, are clearly understood and are sufficiently mitigated.

NERC in collaboration with the industry must address the following questions:

- What will it take to reasonably ensure the reliability of the BPS from a cyber security threat?
- What should NERC do to ensure its efforts are complementary to the efforts of the government and industry with regard to cyber security protection?
- What should NERC do to ensure that there are no “gaps” and no “confusion” with respect to responsibilities for and execution of cyber security protection initiatives?

Overall, NERC is addressing cyber security within each of our major program areas consistent with each program’s scope, unique authority, policies, procedures, and protocols. However, what NERC is currently able to do in each of its programs is limited by a lack of thorough threat analysis and risk assessment. NERC must elevate the importance and sense of urgency associated with cyber security threats, especially as it relates to this shortcoming. While NERC can and will seek to improve in this area, it must also ask “Is it sufficient to continue to treat critical infrastructure protection in the same manner as the remainder of its activities?”

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC, the industry, and the agencies of the respective governments that oversee our reliability activities understand that cyber security threats are not the same as the traditional threats to BPS reliability. NERC cannot be successful going forward without explicitly identifying and addressing the unique challenges that cyber security threats pose to the reliability of the bulk power system.

Security Threats are Jurisdictionally Unbounded

NERC's charter and delegated authority under Section 215 of the Federal Power Act (in the United States) focus on the reliability of the BPS. When Congress drafted Section 215 it intentionally excluded distribution facilities. As a consequence, NERC has no jurisdiction with respect to distribution facilities and it does not require any additional authority over distribution facilities in order to ensure the reliability of the BPS through its reliability standards development and compliance and enforcement program. (Threats of a national security concern could arise from distribution facilities as demonstrated by Aurora but these are outside the charter and delegated authority of NERC.)

Similarly, NERC has no jurisdiction to set or enforce mandatory standards applicable to the providers of telecommunication services and equipment, which also serve as a potential "attack vector" for cyber security threats.

(NERC, in its capacity as the Electric Sector Information Sharing and Analysis Center (ESISAC), also has some related responsibilities for cyber and physical security issues associated with all electric facilities operated in the United States.)

Critical Infrastructure Protection is Ever-changing with Technology

NERC's standards development process is structured to leverage industry subject matter expertise against well defined problems with long histories and defined data; incremental improvement over time can be accepted, rather than quick, significant change without operating experience as a basis and in short timeframes. While the vast majority of our standards apply to the former, cyber security at times requires the latter. Since the technology changes frequently, potential threats arise quickly. SCADA (Supervisory Control and Data Acquisition) and communications technologies continue to evolve at a rapid pace. Standards relating to critical infrastructure in general and cyber-security in particular will need to continue to evolve driving some future change on the industry.

Critical Infrastructure Threats can be Intentional

NERC standards development is designed to respond to defined, measurable risks that can be identified from operating experience, event analysis, compliance audits, system and equipment performance analysis, and benchmarking programs. Consequently the necessity for standards is transparent.

The intentional nature of cyber and physical security threats means the protection of the BPS is dependent in large measure on the quality and timeliness of threat analysis and risk assessments developed by others. Worldwide circumstances rather than operating conditions of the BPS can raise the threat level.

Critical Infrastructure Threats Require Confidential Assessment

NERC draws its technical expertise from the collective wisdom of others who volunteer their time for the good of the cause. When we are successful it is because we assemble these industry subject matter experts into drafting teams, develop and post our proposed standards for broad industry stakeholder comment, and gain approval by supermajority vote.

Unfortunately much of the valuable information on critical infrastructure threats resides within government agencies and confidential treatment of that information is essential. In non-emergency situations coordination with the respective agencies is possible and the limitations associated with confidential information can be mitigated. Nevertheless these are special challenges not required when developing NERC's other reliability standards.

Response (or lack thereof) to Critical Infrastructure Threats can do Harm

As a standard setting and enforcement organization, NERC must do no harm to the reliability of the BPS.

Critical Infrastructure responses to threats are different. Every survey result, every instruction on how to mitigate risks, every documented compliance action comes with some risk of harm because it could provide a road map of actions taken and not taken with respect to protecting the BPS from such threats. Failure to act quickly may cause even greater harm because of the pace of technological change noted above.

Summary

Because cyber security threats are different, NERC must address these threats differently, but consistent with its mission as an international ERO. This is the most compelling reason for change going forward. Recommendations on immediate actions items are outlined below.

Recommendations

1. **Establish a Chief Security Officer (CSO)**

   Recognizing the critical differences associated with cyber security threats to bulk power system reliability, NERC will consolidate responsibility for coordination of cyber security matters across all NERC activities into a single responsibility area. NERC will staff a senior executive to be the "Chief Security Officer" who will serve as a single point of contact for the industry, the Electricity Sector Steering Group (ESSG), and government stakeholders seeking to communicate with NERC on cyber and infrastructure security matters.

2. **Critical Infrastructure Protection as a NERC Program**

Critical Infrastructure Protection must become a higher priority within NERC. To do so we will formally establish a Critical Infrastructure Protection program as one of NERC's statutory functions. The program will be led by the NERC CSO reporting to the NERC CEO with guidance from the ESSG. (The current ESISAC and situation awareness activities may also report to the CSO depending on the successful candidate's qualifications.) The CSO will have responsibility for assuring the Rules of Procedure for all NERC programs are implemented in a timely and effectively manner with respect to Critical Infrastructure Protection. The CSO will be responsible for evaluating and recommending any changes to the rules of procedure necessary to achieve the objectives of the Critical Infrastructure Protection program. The CSO will be responsible for assuring coordination between NERC and the respective government agencies with respect to all critical infrastructure protection matters, especially where confidentiality is an issue. As a first step, the CSO, with the assistance of the regional entities, will perform an assessment, with metrics and recommendations, of the preparedness of the users, owners, and operators on the NERC compliance registry to address cyber security threats. The assessment and recommendations will address preventing intrusions as well as assessing the capability for isolating and limiting attacks so they remain within our abilities to withstand any subsequent equipment losses and restore the system quickly. The CSO should also represent NERC in the Partnership for Critical Infrastructure Security.

3. **Alternative Standard Setting Process for Cyber Security Standards**

As a part of the mandate to the board committee on standards, NERC will establish a task force to review, and where appropriate recommend, a standard setting process for Cyber Security that will include an emergency/crisis standards setting process. This process must provide a level of due process and technical review, but also provide the speed necessary to establish standards quickly and work seamlessly with any new authority granted in the United States to the FERC. NERC will investigate and review standards development models from other industries.

NERC requests the Standards Committee consider the most effective approach for accelerating the review of the existing critical infrastructure protection standards to incorporate the comments from FERC, and specifically consider the extent to which elements of the NIST standards should be included in the NERC cyber security standards.

4. **Improve Depth of Expertise**

NERC will request the Regional Entities who have not already done so to establish a working group of industry experts. Under the direction of the CSO and in consultation with CIPC leadership, NERC will re-examine the charter and scope of the Critical Infrastructure Protection Committee to maximize its contribution to NERC and the industry with respect to cyber security protection. Under the direction of the CSO and director of compliance NERC will increase its IT professional expertise. Regional Entities will be requested to conduct CIP workshops to enhance the development and training of CIP auditors.

NERC will add Critical Infrastructure Protection experience to the search criteria for the next NERC trustee.

5. **Closer Coordination with Government**

NERC, with the guidance of the ESSG, will establish a protocol with DHS, DOE, FERC, and their Canadian counterparts to ensure comprehensive cyber security threat analysis and risk assessment is available to NERC from a consolidated government voice, with industry users, owners, operators able to participate directly.

To ensure NERC is making decisions and setting priorities on the most current information, NERC will, in consultation with FERC, organize a briefing for the ESSG, the NERC CEO, and senior level utility executives across all stakeholder groups on cyber security threats. In particular, NERC will determine the need for, and implement any actions such as, alerts, remedial actions, or urgent and emergency action standards that stem from the briefing.

NERC will work with the ESSG, FERC, and applicable Canadian authorities to identify the most effective and secure method of assessing cyber security preparedness and performance.

6. **Communications**

Under the direction of the CSO, NERC will establish communication protocols for responding to public and media questions on matters associated with Critical Infrastructure Protection, especially with regard to cyber security.

7. **Completion Date**

Completion of these activities in a timely manner is essential. NERC management will report at each board meeting on progress toward these goals with completion of all goals targeted for no later than year end.

Summary

We share a mutual goal — to ensure the reliability of the BPS with respect to cyber security. The recommendations are designed to be complementary to the government as well as users, owners, and operators of the BPS, while making NERC a more effective and responsive organization in regard to security threats to the reliability of the BPS. I welcome your comments and suggestions.

Sincerely,

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Nomination Period Opens for Standard Drafting Team
July 15–28, 2008

The Standards Committee is seeking industry experts to serve on the Cyber Security Standard Drafting Team. This project (Project 2008-06) involves making revisions to the following standards to address FERC's directives in Order 706 and to bring the set of standards into conformance with the ERO Rules of Procedure:

CIP-002-1 — Critical Cyber Asset Identification
CIP-003-1 — Security Management Controls
CIP-004-1 — Personnel & Training
CIP-005-1 — Electronic Security Perimeter(s)
CIP-006-1 — Physical Security of Critical Cyber Assets
CIP-007-1 — Systems Security Management
CIP-008-1 — Incident Reporting and Response Planning
CIP-009-1 — Recovery Plans for Critical Cyber Assets

For this drafting team, the Standards Committee is looking for a variety of expertise, with the possibility of having the team subdivide itself into smaller teams based on expertise.

If you are interested in serving on this drafting team, please use the electronic comment form that is on site below no later than **July 28, 2008.**

http://www.nerc.com/~filez/standards/Project_2008-06_Cyber_Security.html

Please note, we received a very large set of self-nominations from well qualified individuals in response to our request for nominations for the Cyber Security SAR drafting team and were only able to select a small number of people for the SAR drafting team. If you submitted a nomination for the SAR drafting team and are still interested in the project, please do not hesitate to submit a nomination for this standard drafting team. The standard drafting team will be larger than the SAR drafting team. SAR drafting team members will not be automatically selected for the standard drafting team. All nominations submitted for the standard drafting team will be given due consideration.

Standards Development Procedure

The *Reliability Standards Development Procedure Manual* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Nomination Form for Project 2008-06 Cyber Security Order 706 Standard Drafting Team

Please use the electronic nomination form located at the link below to submit your nomination by July 28, 2008. If you have any problems with the form please contact Barbara Bogenrief at Barbara.bogenrief@nerc.net or by telephone at 609-452-8060.

If you have any questions about this project, please contact Scott Mix at scott.mix@nerc.net or by telephone at 215-853-8204.

All candidates should be prepared to participate actively at these meetings.

Name: Organization: Address: Office Telephone: E-mail:
Please briefly describe your experience and qualifications for participating on the standard drafting team for Project 2008-06 Cyber Security Oder 706. Please provide details of your experience, as applicable, related to: • developing or implementing cyber security policies and procedures, • implementing or managing the implementation of the cyber security standards, • implementing substation automation, protection and control, or plant or boiler control systems (this field experience does not need to be security related – it will be used to augment the viewpoints of the drafting team to provide more realistic and practical modifications to the standards) • previous experience working on or applying NIST standards • experience writing compliance elements in support of NERC standards. NERC staff will use the information provided as the basis for developing a recommendation to the Standards Committee for the standard drafting team for Project 2008-06 Cyber Security Oder 706. It is very important that the information you provide be concise and clearly indicate why you feel you are qualified to participate on this team. If you are selected, which standards drafting subteam(s) do you prefer? ☐ Drafting requirements ☐ Drafting compliance elements

Indicate all NERC Reliability Region(s) in which your company operates :	**Indicate all Industry Segments in which your company has a Registered Ballot Body representative:**	
☐ ERCOT ☐ FRCC ☐ MRO ☐ NPCC ☐ RFC ☐ SERC ☐ SPP ☐ WECC ☐ NA – Not Applicable	☐	1 — Transmission Owners
	☐	2 — RTOs, ISOs
	☐	3 — Load-serving Entities
	☐	4 — Transmission-dependent Utilities
	☐	5 — Electric Generators
	☐	6 — Electricity Brokers, Aggregators, and Marketers
	☐	7 — Large Electricity End Users
	☐	8 — Small Electricity End Users
	☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities

Indicate all Function(s)[1] in which you have expertise or responsibilities:

☐ Balancing Authority	☐ Planning Coordinator
☐ Compliance Monitor	☐ Transmission Operator
☐ Distribution Provider	☐ Transmission Owner
☐ Generator Operator	☐ Transmission Planner
☐ Generator Owner	☐ Transmission Service Provider
☐ Interchange Authority	☐ Purchasing-selling Entity
☐ Load-serving Entity	☐ Resource Planner
☐ Market Operator	☐ Reliability Coordinator

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group.

Name:	Office Telephone:
Organization:	E-mail:
Name:	Office Telephone:
Organization:	E-mail:

[1] These functions are defined in the NERC Functional Model, which is downloadable from the NERC Web site.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Comment Period Open
November 21, 2008–January 5, 2009

Now available at:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

First Draft of Revised Cyber Security Standards CIP-002-1 through CIP-009-1 (Project 2008-06)

The Cyber Security Standard Drafting Team has posted its first drafts of revisions to cyber security standards CIP-002-1 through CIP-009-1 and associated implementation plans for a 45-day comment period. The comment period is now **open until 8 p.m. on January 5, 2009.**

The drafting team has been assigned the responsibility of revising the cyber security standards as follows:

- ensure the standards conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure
- address the directed modifications identified in FERC Order 706
- consider other cyber-related standards, guidelines, and activities

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at 609-452-8060.

The status, purpose, and supporting documents for this project — including an off-line, unofficial copy of the questions listed in the comment form — are posted at the following site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–002–2 — Cyber Security — Critical Cyber Asset Identification and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

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

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its dated list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its dated list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its dated approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification

2. **Number:** CIP-002-1~~2~~

3. **Purpose:** NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

   - **4.1.1** Reliability Coordinator.
   - **4.1.2** Balancing Authority.
   - **4.1.3** Interchange Authority.
   - **4.1.4** Transmission Service Provider.
   - **4.1.5** Transmission Owner.
   - **4.1.6** Transmission Operator.
   - **4.1.7** Generator Owner.
   - **4.1.8** Generator Operator.
   - **4.1.9** Load Serving Entity.
   - **4.1.10** NERC.
   - **4.1.11** Regional ~~Reliability Organizations~~Entity.

   4.2. The following are exempt from Standard CIP-002-2:

   - **4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
   - **4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. **Effective Date:** ~~June~~ ~~The later of: a)~~ tThe first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)~~; or b) compliant dates (C) identified in~~

the compliance schedule of the implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1.

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-002:~~

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — ~~A~~ The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:~~

M1. ~~The~~ Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its dated list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its dated list of Critical Cyber Assets as specified in Requirement R3.

M4. ~~The~~The Responsible Entity shall make available its dated approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~ Compliance Enforcement Authority in conjunction with the Registered Entity~~Responsible Entity~~ shall keep the last audit records and all requested and submitted subsequent audit records.~~for three calendar years.~~

1.5. Additional Compliance Information

1.5.1 ~~Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor~~None.

2. ~~Levels of Non-Compliance~~Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

~~2.1 Level 1:~~ ~~The risk assessment has not been performed annually.~~

~~2.2 Level 2:~~ ~~The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.~~

~~2.3 Level 3:~~ ~~The list of Critical Assets or Critical Cyber Assets does not exist.~~

~~2.4 Level 4:~~ ~~The lists of Critical Assets and Critical Cyber Assets do not exist.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–003–2 — Cyber Security – Security Management Controls and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

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

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-1~~2~~

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

~~**4.1.11**Regional Reliability Organizations.~~

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

5. Effective Date: ~~June~~ ~~The later of: a)~~ tThe first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)~~; or b) compliant dates (C) identified in the compliance schedule of the implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1~~.

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-003:~~

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, ~~business phone, business address,~~ and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations ~~must~~shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures~~, or a statement accepting risk~~.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or ~~-~~delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements~~ Responsible Entity shall make available documentation of ~~Standard CIP-003:~~

M1. ~~Documentation of the Responsible Entity's~~its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. ~~Documentation~~ The Responsible Entity shall make available documentation of the assignment of, and changes to, ~~the Responsible Entity's~~its leadership as specified in Requirement R2.

M3. ~~Documentation of the Responsible Entity's~~ The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. ~~Documentation of the~~The Responsible ~~Entity's~~Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible ~~Entity's~~Entity shall make available ~~-~~its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

1.1.1 Regional Reliability OrganizationsEntity for Responsible Entities.

1.1.1 NERC that do not perform delegated tasks for their Regional Reliability OrganizationEntity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The compliance monitorThe Responsible EntityCompliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. for three years.

1.5. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

~~2.2. Level 2:~~

~~2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,~~

~~2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,~~

~~2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,~~

~~2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.~~

~~2.3. Level 3:~~

~~2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,~~

~~2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,~~

~~2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.~~

~~2.4. Level 4:~~

~~2.4.1 No cyber security policy exists; or,~~

~~2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,~~

~~2.4.3 No documented change control and configuration management process exists.~~

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities	

		which have no Critical Cyber Assets. Changed compliance monitor to ~~Responsible Entity~~Compliance Enforcement Authority. ~~to keep audit records.~~	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–002–4 — Cyber Security — Personnel and Training and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-2

3. Purpose: Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

A. Requirements

R1. Awareness — The Responsible Entity shall establish, maintain, document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);

- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, maintain, document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be annually reviewed and updated as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

B. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

D. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Removal of 90 day window to complete training and personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-1~~2~~

3. Purpose: Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-004-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June~~ ~~The later of: a)~~ tThe first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)~~; or b) compliant dates (C) identified in the compliance schedule of the implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1~~.

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-004:~~

R1. Awareness — The Responsible Entity shall establish, maintain, ~~and~~ document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

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

R2. Training — The Responsible Entity shall establish, maintain, ~~and~~ document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets~~, and review the~~. The cyber security training program shall be annually reviewed and ~~update~~updated as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained ~~within ninety calendar days of~~prior to their being granted such ~~authorization~~access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program ~~within thirty days of~~prior to such personnel being granted such access~~. Such~~ except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the

access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:~~

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. ~~Documentation of the~~The Responsible ~~Entity's~~Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. ~~Documentation~~The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. ~~Documentation~~The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The ~~compliance monitor~~~~Responsible Entity~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.~~for three calendar years.~~

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.~~

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~**2.1.1** Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,~~

~~**2.1.2** Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,~~

~~**2.1.3** Personnel risk assessment program exists, but documentation of that program does not exist; or,~~

~~**2.1.4** List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.~~

~~**2.1.5** One personnel risk assessment is not updated at least every seven years, or for cause; or,~~

~~**2.1.6** One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.~~

~~2.2. Level 2:~~

~~**2.2.1** Awareness program does not exist or is not implemented; or,~~

~~**2.2.2** Training program exists, but does not address the requirements identified in Standard CIP-004; or,~~

~~**2.2.3** Personnel risk assessment program exists, but assessments are not conducted as required; or,~~

~~**2.2.4** One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.~~

~~2.3. Level 3:~~

~~2.3.1 Training program exists, but has not been reviewed and updated at least annually; or,~~

~~2.3.2 A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,~~

~~2.3.3 List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.~~

~~2.4. Level 4:~~

~~2.4.1 No documented training program exists; or,~~

~~2.4.2 No documented personnel risk assessment program exists; or,~~

~~2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.~~

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel termination for cause…”	03/24/06
1	06/01/06	D.2.1.4 — Change “access control rights” to “access rights.”	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Removal of 90 day window to complete training and personnel risk assessments. Changed compliance monitor to ~~Responsible Entity to keep audit records~~Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–005–2 — Cyber Security — Electronic Security Perimeter(s) and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

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

2. Number: CIP-005-2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; and,

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

M1. The Responsible Entity shall make available dated documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available dated documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available dated documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available dated documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available dated access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity.	

		Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

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

2. Number: CIP-005-~~1~~2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations.~~Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June~~ ~~The later of: a) t~~The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required)~~; or b) compliant dates (C) identified in the compliance schedule of the implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1~~.

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-005:~~

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003~~,~~-2; Standard CIP-004-2 Requirement R3~~,~~; Standard CIP-005-2 Requirements R2 and R3~~,~~; Standard CIP-006 ~~Requirements R2 and~~ -2 Requirement R3~~,~~; Standard CIP-007~~,~~-2 Requirements R1 and R3 through R9~~,~~; Standard CIP-008~~,~~-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; and,

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-005.~~ Responsible ~~entities may document controls either individually or by specified applicable grouping.~~

M1. ~~Documents~~Entity shall make available dated documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. ~~Documentation of~~ The Responsible Entity shall make available dated documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. ~~Documentation~~The Responsible Entity shall make available dated documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. ~~Documentation of the Responsible Entity's~~The Responsible Entity shall make available dated documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. ~~Access~~The Responsible Entity shall make available dated access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The ~~compliance monitor~~~~Responsible Entity~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. ~~for three years.~~

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior~~

manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

~~2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,~~

~~2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,~~

~~2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.~~

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to ~~Responsible Entity to keep audit records~~Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–006–2 — Cyber Security — Physical Security and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-2

3. Purpose: Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-006-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, maintain, and implement a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation..

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	

A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets

2. **Number:** CIP-006-12

3. **Purpose:** Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Reliability OrganizationsEntity.

   4.2. The following are exempt from Standard CIP-006-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. **Effective Date:** June The later of: a) tThe first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required); or b) compliant dates (C) identified in the compliance schedule of the Implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1.

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

R1. Physical Security Plan — The Responsible Entity shall create and document, maintain, and implement a physical security plan, approved by a the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that allAll Cyber Assets within an Electronic Security Perimeter also shall reside within an identified Physical Security Perimeter.

Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Criticalsuch Cyber Assets.

R1.2. Processes to identify Identification of all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriateAppropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewingReview of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Procedures forContinuous escorted access within the physical security perimeterPhysical Security Perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating Update of the physical security plan within ninetythirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeterPhysical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets used in thethat authorize and/or log access control and monitoring ofto the Physical Security Perimeter(s)), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall be:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006 Requirement R2 and R3,-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

R3.0. Process for ensuring that the physical security plan is reviewed at least annually.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

P4.1.• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

P4.2.• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

P4.3.• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

~~P4.4.~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

~~P5.1.~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

~~P5.2.~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement ~~R2.3~~R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

~~P6.1.~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

~~P6.2.~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity.

~~P6.3.~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement ~~R2.3~~R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements ~~R2, R3~~R4, R5, and ~~R4~~R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement ~~R6~~R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

~~The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:~~

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. ~~Documentation~~The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2R4.

M5. DocumentationThe Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R3R5.

M6. DocumentationThe Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R4R6.

M7. AccessThe Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R5R7.

M8. DocumentationThe Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R6.R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1. Compliance Enforcement Authority

1.1.1 Regional Reliability OrganizationsEntity for Responsible Entities.

1.1.1 NERC that do not perform delegated tasks for their Regional Reliability OrganizationEntity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements ~~R5~~R7 and ~~R6~~R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation..

1.4.2 The ~~compliance monitor~~~~Responsible Entity~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. ~~for three calendar years.~~

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.~~

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

~~2.~~ Violation Severity Levels ~~of Noncompliance~~

~~**2.1. Level 1:**~~

2. ~~The physical security plan exists, but has not been updated within ninety calendar days of a modification to~~**(Under development by the** ~~plan or any of its components; or,~~**CIP VSL Drafting Team)**

~~**2.1.2** Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~**2.1.3** Required documentation exists but has not been updated within ninety calendar days of a modification.; or,~~

~~**2.1.4** Physical access logs are retained for a period shorter than ninety days; or,~~

~~**2.1.5** A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,~~

~~**2.1.6** One required document does not exist.~~

~~**2.2. Level 2:**~~

~~**2.2.1** The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,~~

~~**2.2.2** Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~**2.2.3** Required documentation exists but has not been updated within six calendar months of a modification; or~~

~~**2.2.4** More than one required document does not exist.~~

~~**2.3. Level 3:**~~

~~2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,~~

~~2.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~2.3.3 No logs of monitored physical access are retained.~~

~~2.4. Level 4:~~

~~2.4.1 No physical security plan exists; or,~~

~~2.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~2.4.3 No maintenance or testing program exists.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed	

		from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–007–2 — Cyber Security — Systems Security Management and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date.	

		R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-1~~2~~

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the ~~non-critical~~other Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June~~ The ~~later of: a) the~~ first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)~~; or b) compliant dates (C) identified in the compliance schedule of the implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1~~.

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):~~

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service

packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish and , document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish and , document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~thirty calendar days of the change being completed.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:~~

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. ~~Documentation~~The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. ~~Documentation~~The Responsible Entity shall make available documentation and records of ~~the Responsible Entity's~~its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. ~~Documentation~~The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The ~~compliance monitor~~~~Responsible Entity~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. ~~for three calendar years.~~

1.5. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or

2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,

2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
- Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

~~2.2. Level 2:~~

~~2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.3. Level 3:~~

~~2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4. Level 4:~~

~~2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4.3 No logs exist.~~

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to ~~Responsible Entity to keep audit records~~Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–008–2 — Cyber Security — Incident Reporting and Response Planning and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-2

3. Purpose: Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its dated Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-~~1~~2

3. **Purpose:** Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. **Applicability**

   4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional ~~Reliability Organizations~~Entity.

   4.2. The following are exempt from Standard CIP-008-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. **Effective Date:** ~~June~~ The ~~later of: a) the~~ first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)~~; or b) compliant dates (C) identified in the compliance schedule of the implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1~~.

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-008:~~

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident ~~Response~~response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of ~~incident~~Cyber Security Incident response teams, ~~incident~~Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES~~–~~ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES~~–~~ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the ~~incident~~Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of CIP-008:~~

M1. ~~The~~ Responsible Entity shall make available its dated Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan

M2. ~~All~~The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ ~~Regional Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~~~Responsible Entity~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. ~~for three calendar years.~~

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.~~

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

~~**2.** **Violation Severity Levels of Noncompliance**~~

~~**2.1. Level 1:** A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.~~

~~**2.2. Level 2:**~~

~~**2.2.1** A Cyber Security Incident response plan exists, but has not been reviewed in~~**(Under Development by the** ~~previous full calendar year; or,~~

~~**2.2.2** A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,~~

~~**2.2.3** Records related to reportable Cyber Security Incidents were not retained for three calendar years.~~

~~**2.3. Level 3:**~~

2. ~~A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard~~ **CIP**~~-008; or,~~ **VSL Drafting Team)**

~~**2.3.2** A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.~~

~~**2.4. Level 4:** A Cyber Security Incident response plan does not exist.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to ~~Responsible Entity to keep audit records~~Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-2

3. Purpose: Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its dated recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its dated records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its dated documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its dated documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its dated documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-~~1~~2

3. Purpose: Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional ~~Reliability Organizations~~Entity

4.2. The following are exempt from Standard CIP-009-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June~~ The ~~later of: a) the~~ first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)~~; or b) compliant dates (C) identified in the compliance schedule of the implementation Plan for Cyber Security Standards CIP-002-1, 2006 through CIP-009-1~~.

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:~~

M1. ~~Recovery~~Responsible Entity shall make available its dated recovery plan(s) as specified in Requirement R1.

M2. ~~Records~~The Responsible Entity shall make available its dated records documenting required exercises as specified in Requirement R2.

M3. ~~Documentation of~~ The Responsible Entity shall make available its dated documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. ~~Documentation~~The Responsible Entity shall make available its dated documentation regarding backup and storage of information as specified in Requirement R4.

M5. ~~Documentation~~The Responsible Entity shall make available its dated documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.3.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year .

1.3.2 The unless directed by its Compliance MonitorEnforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible EntityCompliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. for three calendar years.

1.5. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,~~

~~2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.~~

~~2.2. Level 2:~~

~~2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,~~

~~2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.~~

~~2.3. Level 3:~~

~~2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,~~

~~2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.~~

~~2.4. Level 4:~~

~~2.4.1 No recovery plan(s) exist; or,~~

~~2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.~~

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judg~~e~~ment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to ~~Responsible Entity to keep audit records~~Compliance Enforcement Authority.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Modified Standards

The following standards have been modified:
CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

Red-line versions of the above standards are posted with this Implementation Plan. When these modified standards become effective, the prior versions of these standards and their Implementation Plan are retired.

Compliance with Standards

Once these standards become effective, the responsible entities identified in the Applicability section of the standard must comply with the requirements. These include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.

Proposed Effective Date

The proposed effective date for these modified standards is the first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

Implementation Plan for Cyber Security Standards CIP-003-1 through CIP-009-1 or Their Successor Standards

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan identifies the schedule for becoming compliant with the requirements of NERC Standards CIP-003-1 through CIP-009-1 and their successor standards, for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed.

This Implementation Plan specifies only a 'Compliant' milestone. The Compliant milestone is expressed in this Implementation Plan table (Table 2) as the number of months following the designation of the newly identified asset as a Critical Cyber Asset, following the requirements of NERC Standard CIP-002-1 or its successor standard.

For some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as '0' herein. For other requirements, the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date. These are annotated as *existing*.

In all cases where a milestone for compliance is specified (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the milestone listed in this Implementation Plan. Where the milestone assumes prior compliance (i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones.

There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.

Implementation Schedule

There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:

1. A Cyber Asset becomes the *first identified* Critical Cyber Asset at a responsible Entity. No existing CIP compliance program for CIP-003 through CIP-009 is assumed to exist at the Responsible Entity.
2. An existing Cyber Asset becomes subject to CIP standards, *not due to planned change*. A CIP compliance program already exists at the Responsible Entity.
3. A new or existing Asset becomes subject to CIP standards *due to planned change*. A CIP compliance program already exists at the Responsible Entity.

Note that the term 'Cyber Asset becomes subject to the CIP standards' applies to all Critical Cyber Assets, as well as non-critical Cyber Assets within an Electronic Security Perimeter.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

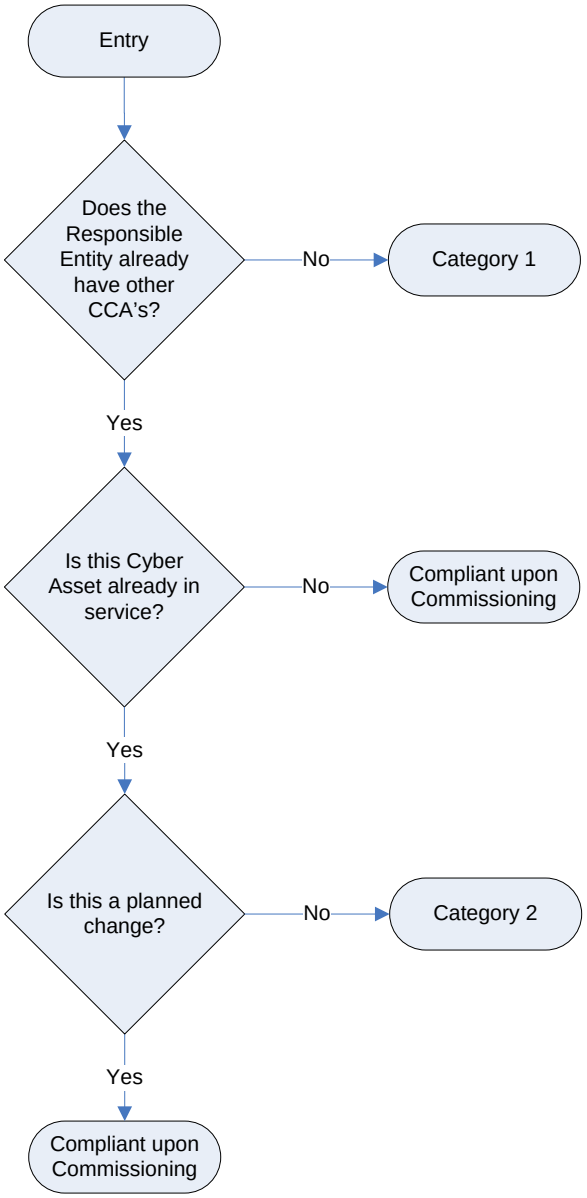

Figure 1: Category Selection Process Flow

The individual categories are distinguished as follows:

1. **Category 1**: A Responsible Entity that previously has undergone the CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-003-1 through CIP-009-1.) As such, it is presumed that the Responsible Entity has no previously established cyber security program in force. Table 3 also shall apply in the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.

2. **Category 2**: A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule, and now has added additional items to its Critical Cyber Asset list. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented. Since the Responsible Entity already has a CIP compliance program, it needs only to implement the CIP standards for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement.

   In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.

   In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.

3. **Compliant upon Commissioning**: When a Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant

when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset upon its commissioning or activation (e.g., based on planning or impact studies).
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security perimeter) associated with a previously identified Critical Asset.
c) Addition of:
    i. a Critical Cyber Asset, or,
    ii. an other (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset where that Entity has an established CIP Compliance Program as required by an existing Implementation Schedule.

This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

Since the assets must be compliant upon commissioning, no milestones are provided herein.

Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards.

As an example, Table 1 provides some sample situations, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Program:	
	No CIP Program (note 1)	Existing CIP Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset - never before in service and not a replacement for an existing Cyber Asset - added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as a non-critical asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24	*existing*
R2	1	*existing*
R3	24	*existing*
R4	24	*existing*
R5	24	*existing*
R6	24	*existing*
Standard CIP-004-2 — Personnel and Training		
R1	24	*existing*
R2	24	6
R3	24	6
R4	24	6
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24	12
R2	24	12
R3	24	12
R4	24	12
R5	24	12
Standard CIP-006-2 — Physical Security		
R1	24	12
R2	24	12
R3	24	12
R4	24	12
R5	24	12
R6	24	12

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24	12
R2	24	12
R3	24	12
R4	24	12
R5	24	12
R6	24	12
R7	24	12
R8	24	12
R9	24	12
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24	6
R2	24	0
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24	6
R2	24	0
R3	24	0
R4	24	6
R5	24	6

Table 3[1] Compliance Schedule for Standards CIP-002-1 through CIP-009-1 or Their Successor Standards For Entities Registering in 2008 and Thereafter				
	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	**All Facilities**	**All Facilities**	**All Facilities**	**All Facilities**
CIP-002-1 Critical Cyber Assets or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-003-1 — Security Management Controls or its Successor Standard				
All Requirements Except R2	**BW**	**SC**	**C**	**AC**
R2	**SC**	**C**	**AC**	**AC**
Standard CIP-004-1 — Personnel & Training or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-005-1 — Electronic Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-006-1 — Physical Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-007-1 — Systems Security Management or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-008-1 — Incident Reporting and Response Planning or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-009-1 — Recovery Plans or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**

[1] The phase in of compliance in this table is identical to the phase in for CIP-002-1 through CIP-009-1 identified in Table 4 of the 2006 CIP Implementation Plan.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comment Form for Phase I of Project 2008-06 — Cyber Security Order 706

Please use the electronic comment form located at the link below to submit comments on the proposed revisions of CIP-002-1 through CIP-009-1, developed by the standard drafting team as part of Project 2008-06 — Cyber Security Order 706. Comments must be submitted by **January 5, 2009**. If you have questions please contact Harry Tom at Harry.Tom@nerc.net or by telephone at (860) 550-4157.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Background Information

On July 10th, 2008, the NERC Standards Committee approved the Standard Authorization Request (SAR) for developing revisions to the following Critical Infrastructure Protection Cyber Security standards:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

A Standards Drafting Team (SDT) was appointed by the Standards Committee on August 7, 2008 to develop these revisions as part of Project 2008-06 — Cyber Security Order 706. The SDT for Project 2008-06 has been assigned the responsibility to review each of the reliability standards identified above to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706. In conjunction with the project, the SDT will also consider other cyber-related standards, guidelines and activities:

- The National Institute of Standards and Technology (NIST) Security Risk Management Framework [includes General Accounting Office (GAO), Office of Management and Budget (OMB) and Federal Information Processing Standards (FIPS)].
- Other cyber security related documents such as NIST, International Organization for Standardization (ISO) 27000 Family, Critical Infrastructure Protection Committee (CIPC) Risk Assessment Guideline, MITRE corporation technical report, Department of Homeland Security (DHS), National Laboratories papers, Department of Energy (DOE) 417, International Electrotechnical Commission (IEC), International Society of Automation (ISA), etc.
- Coordination work between FERC, Nuclear Energy Institute (NEI) and Nuclear Regulatory Commission (NRC) in regard to the nuclear facility exemption issue with respect to regulatory gaps and modify, as necessary, the standards to reflect current determinations.

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Revisions will consider additional issues identified by stakeholders in the SAR comment process. Issues are listed in the SAR at http://www.nerc.com/docs/standards/sar/SAR_Modify_CIP_Stds_D2_clean_07Jul08.pdf and http://www.nerc.com/docs/standards/sar/SAR_Attach2_Order_706_Analysis.pdf (two files).

The SDT met on October 6–8, 2008 and because of the extensive scope and varying complexity of the issues and work in these revisions, the team decided on a multiphase approach for revising this set of standards. This posting of the cyber standards for industry comment only relates to Phase I of the project.

Summary of Phase I Revisions

Phase I includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I modifications and are outlined below. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase of Project 2008-06 — Cyber Security Order 706.

The following provides a brief summary of the proposed modifications to this set of standards as Phase I of Project 2008-06 — Cyber Security Order 706. For All CIP 002-1— CIP 009-1 Standards the following modifications are proposed:

- As directed in Order 706
  - Purpose Section: Removed the term "reasonable business judgment".
  - Where applicable, removed the phrase "acceptance of risk".
- To comply with ERO Rules of Procedure
  - Applicability: Added Regional Entity in place of Regional Reliability Organization.
- Versioning
  - Phase I changes to the existing version will be reflected as CIP 002–2 through CIP 009–2.
- Effective Date section updated to integrate the implementation timeframe for CIP 002–2 through CIP 009–2.
- Administrative edits to reflect changes in numbering references.
- Requirements
  - Where there were sub-requirements that were numbered, but were not all required, the numbers were replaced with "bullets".
- Measures
  - The format of the measures was modified to conform to the format used in other standards.
- Compliance Elements
  - The compliance elements of the standard were updated to reflect the language used in the ERO Rules of Procedure.
  - The term, "Compliance Monitor" was replaced with "Compliance Enforcement Authority".

- The term, "Regional Reliability Organization" was replaced with "Regional Entity".
- The Compliance Monitoring and Enforcement Processes were added.
- The Monitoring Time Period and Reset Periods were marked as "not applicable".
- The Data Retention section was updated.

In addition to the changes noted above, the following modifications are proposed to apply to specific CIP standards as noted below:

CIP 002 Modifications

- As directed in Order 706
  - R4 Annual Approvals: Adds that the senior manager shall annually review and approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets as required in prior version.

CIP 003 Modifications

- Simplification
  - R2.1 Leader Identification: Removes the need for business phone and business address designation.
- As directed in Order 706
  - Applicability 4.2.3: Requires Responsible Entities having no Critical Cyber Assets to comply with CIP 003-2 R2.
  - R2 Leadership: Require the designation of a single manager, with overall responsibility and authority for leading and managing the entity's implementation of CIP. The word "authority" is an addition.
  - R2.3: Permits the assigned senior manager to delegate authority in writing for specific actions, where allowed, throughout the CIP standards.

CIP 004 Modifications

- Clarification to assure that requirement must be implemented
  - R1. Awareness: Explicitly requires implementation of Awareness Program.
  - R2. Training: Explicitly requires implementation of the Training Program.
- As directed in Order 706
  - R2.1 Training: Personnel having access to Critical Cyber Assets must be trained prior to their being granted such access, except in specified circumstances, such as an emergency. This replaces allowance for ninety days to complete the training and adds provision for emergency situations.
  - R3 Personnel Risk Assessment: Personnel risk assessment shall be conducted prior to granting personnel access to Critical Cyber Assets except in specified circumstances such as an emergency. This replaces allowance for thirty days to complete personnel risk assessment and adds provision for emergency situation.

CIP 005 Modifications

- Clarification
  - Clarifies the scope of this requirement to include Cyber Assets used in either access control and/or monitoring to the Electronic Security Perimeter.
- Clarification to assure that requirement must be implemented
  - R2.3 Electronic Access Controls: Explicitly requires the implementation of the procedure to secure dial up access to the Electronic Security Perimeter.

CIP 006 Modifications

- Restructuring of Requirements
  - Former requirement R1.8 moved and incorporated into new Requirement R2 (Protection of Physical Access Control Systems) as Requirement R2.2.
  - Other modifications to Requirements R1.1 through R1.8 for readability.
- Clarifications to assure that requirement must be implemented
  - R1.–R1.8 Physical Security Plan: All requirements of the Physical Security Plan must be implemented.
- Additional Clarifications
  - R1.6 Escorted Access: Clarified that the escort within a Physical Security Perimeter should continually remain with the escorted person.
  - R1.8 Annual Review: Formerly Requirement R1.9.
  - R2.2: Formerly R1.8. Changed references to requirement numbers as appropriate.
  - R4 Physical Access Controls: Formerly Requirement R2. Changes enumeration of sub requirements to bulleted list.
  - R5 Monitoring Physical Access: Formerly Requirement R3. Changes enumeration of sub requirements to bulleted list. Changes references to other requirements as appropriate.
  - R6 Logging Physical Access: Formerly Requirement R4. Changes enumeration of sub requirements to bulleted list. Changes references to other requirements as appropriate.
  - Requirement R7: Formerly Requirement R5.
  - R8 Maintenance and Testing: Formerly Requirement R6. Changes references to other requirements as appropriate.
- As directed in Order 706
  - R1.7 Updates to the Physical Security Plan: Shortens the time for updates to the Physical Security Plan to thirty calendar days rather than ninety days and adds the word “completion” to the requirement.
  - R1 Physical security Plan: Changes the term “a senior manager” to “the senior manager.”
- Requirements Added
  - R2 Protection of Physical Access Control Systems: Moves requirement to protect Physical Access Control Systems out of Requirement R1 into its own requirement and excludes hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers from the requirement.
  - R2.1 Protection of Physical Access Control Systems: Adds requirement that Physical Access Control Systems be protected from unauthorized access.
  - R3 Protection of Electronic Access Control Systems: Adds that cyber assets used in access control and/or monitoring of the Electronic Security Perimeter shall reside within an identified Physical Security Perimeter.

CIP 007 Systems Security Management Modifications

- As directed in Order 706
  - R2.3 Ports and Services: Removal of the term “or an acceptance of risk.”
  - R3.2 Security Patch Mgt.: Removal of the term “or an acceptance of risk.”
  - R4.1 Malicious Software Prevention: Removal of the term “or an acceptance of risk.”

  - R9 Documentation Review and Maintenance: Shortens the time frame to update documentation in response to a system or control change from ninety to thirty calendar days and further clarifies this timeframe to begin after such change is complete.

- Clarifications to assure that requirements must be implemented
  - R2 Ports and Services: Explicitly requires the implementation of process to ensure only required ports and services are enabled.
  - R3 Security Patch Mgt.: Explicitly requires the implementation of Security Patch Management program.
  - R7 Disposal and Redeployment: Explicitly requires the implementation of Cyber Asset disposal and redeployment procedures.

CIP 008 Incident Response & Reporting Modifications

- As directed in Order 706
  - R1.4 Updating the Cyber security Incident Response Plan: Shortens the timeframe to update the Incident Response Plan from ninety to thirty calendar days.
  - R1.6 Testing of the Incident Response Plan: Adds language to clarify that testing need not require a responsible entity to remove any systems from service.
- Clarifications to assure that requirements must be implemented
- R1 Incident Response Plan: Explicitly requires implementation.

CIP 009 Recovery Plan Modifications

- As directed in Order 706
  - R3 Change Control: Shortens the timeframe for communicating updates to Critical Cyber Asset recovery plans from within ninety to thirty calendar days of the change being completed.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

The CSO706 SDT proposes an implementation plan to address newly identified Critical Cyber Assets. Three specific classes of categories for newly identified Critical Cyber Assets are described. The plan provides an implementation schedule with “Compliant” milestones for each requirement in each category. All timelines are specified as an offset from the date when the Critical Cyber Asset has been newly identified.

Questions

Your responses to the following questions will assist the SDT for Project 2008-06 Cyber Security Order 706 (CSO706 SDT) in finalizing the Phase I work for CIP-002-2 through CIP-009-2 relative to the proposed modifications summarized above. For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

You do not have to answer all questions. Enter All Comments in Simple Text Format.

Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.

1. The CSO706 SDT added management approval of the risk-based assessment methodology (per FERC Order 706, paragraph 236) to CIP-002-1 Requirement R4.

   Do you agree with the proposed modification? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

   ☐ Yes

   ☐ No

   Comments:

2. The CSO706 SDT is proposing the following modifications to CIP-003-1:

   - Revise Applicability 4.2.3 to specify that compliance with Requirement R2 applies to Responsible Entities that have determined they have no Critical Cyber Assets (per FERC Order 706, paragraph 376).
   - Clarify the intent of the Requirement R2 on Leadership that a senior manager be assigned with the overall responsibility and authority for cyber security matters (per FERC Order 706, paragraph 381).
   - Add Requirement R2.3 to address senior manager delegation of authority for specific actions to a named delegate.
   - Renumber the original R2.3 to R2.4.
   - Delete the phrase "or a statement accepting risk" from Requirement R3.2.(per FERC Order 706, paragraph 376)

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

   ☐ Yes

   ☐ No

   Comments:

3. The CSO706 SDT is proposing the following modifications to CIP-004-1:

   - In R1 and R2, clarify the requirement to implement security awareness and annual cyber security training programs.
   - Revise R2.1 to train personnel prior to granting access (per FERC Order, paragraph 431).
   - Revise R3 to complete a personnel risk assessment prior to granting access (per FERC Order, paragraph 443).
   - In Requirements R2.1 and R3, the SDT adopted the FERC Order 706 language, "except in specified circumstances such as an emergency," to address unusual events that demand urgent action before the personnel risk assessment can be completed.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

☐ Yes

☐ No

Comments:

4. The CSO706 SDT is proposing the following modifications to CIP-005-1:

   - In R1.5, clarify the requirement to safeguard Cyber Assets used in the control or monitoring of Electronic Security Perimeter.
   - The term "implement" was added to CIP-005-1 Requirement R2.3 to clarify that the procedure for securing dial-up access to the Electronic Security Perimeter must be both maintained and implemented.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

   ☐ Yes

   ☐ No

   Comments:

5. The CSO706 SDT is proposing the following modifications to CIP-006-1:

   - Clarify Requirement R1 that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. CIP-006-1 Requirements R1.1 through R1.7 and R1.9 were revised to clarify the elements that, at a minimum, must be addressed in the physical security plan.
   - The SDT added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2.
   - The SDT added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter.
   - Subsequent Requirements were renumbered and references were appropriately revised. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to lists of options consistent with the intent of the requirements.
   - The SDT revised the Measures to add "implementation" to Measure M1 documentation elements for Requirement R1, added Measure M2 to document the protection of physical access control systems, added Measure M3 to document the protection of electronic access control systems, and renumbered

subsequent Measures and references to Requirements. The SDT also added failure to implement the security plan as Level 4 non-compliance.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

☐ Yes

☐ No

Comments:

6. The CSO706 SDT is proposing the following modifications to CIP 007-1:

- Add "implement" to CIP-007-1 Requirements R2, R3 and R7 to clarify that processes and procedures must be implemented as well as documented.
- Remove the "acceptance of risk" language (per FERC Order 706, paragraph 622) in Requirements R2.3, R3.2 and R4.1.
- Revise the timeframe for documenting changes to systems or controls to thirty days in Requirement R9.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

☐ Yes

☐ No

Comments:

7. The CSO706 SDT modified CIP-008-1 Requirement R1 to clarify the requirement to implement the plan in response to cyber security incidents, update the plan within thirty days of any changes, and clarify that tests of the plan do not require removing components or systems during the test.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

☐ Yes:

☐ No

Comments:

8. The CSO706 SDT revised the timeframe to thirty days for communicating updates of recovery plans to personnel responsible for activating or implementing the plan in CIP-009-1 Requirement R3.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

☐ Yes

☐ No

Comments:

9. The CSO706 SDT proposes the following for the Effective Date:

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

   Do you agree with the proposed Effective Date? If not, please explain and provide an alternative to the proposed effective date that would eliminate or minimize your disagreement.

   ☐ Yes

   ☐ No

   Comments:

10. The CSO706 SDT is proposing a separate CIP implementation plan to address newly identified Critical Cyber Assets. In this plan, three specific classes of categories for newly identified Critical Cyber Assets are described. The plan provides an implementation schedule with "Compliant" milestones for each requirement in each category. All timelines are specified as an offset from the date when the Critical Cyber Asset has been newly identified.

    Do you agree with the approach proposed by the SDT for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement.

    ☐ Yes

    ☐ No

    Comments:

11. Do you agree with the compliance milestones included in the proposed implementation plan for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement.

    ☐ Yes

    ☐ No

    Comments:

12. The CSO706 SDT seeks input on whether to include the information contained in this stand-alone implementation plan within the body of each standard. This would likely

entail a new requirement in CIP-002 to classify newly identified Critical Cyber Assets, and changes to the remaining standards to insert the milestone timeframes.

Do you agree with including the information about newly identified Critical Cyber Assets and newly registered entity information within the body of the standards which would eliminate the stand-alone documents? If not, please explain.

☐ Yes

☐ No

Comments:

13. Do you agree that the Phase I improvements addresses the time-sensitive FERC Order directives? If not, please explain.

☐ Yes

☐ No

Comments:

Individual or group. (48 Responses)
Name (30 Responses)
Organization (30 Responses)
Group Name (18 Responses)
Lead Contact (18 Responses)
Contact Organization (18 Responses)
Question 1 (47 Responses)
Question 1 Comments (48 Responses)
Question 2 (46 Responses)
Question 2 Comments (48 Responses)
Question 3 (44 Responses)
Question 3 Comments (48 Responses)
Question 4 (45 Responses)
Question 4 Comments (48 Responses)
Question 5 (44 Responses)
Question 5 Comments (48 Responses)
Question 6 (44 Responses)
Question 6 Comments (48 Responses)
Question 7 (45 Responses)
Question 7 Comments (48 Responses)
Question 8 (47 Responses)
Question 8 Comments (48 Responses)
Question 9 (44 Responses)
Question 9 Comments (48 Responses)
Question 10 (43 Responses)
Question 10 Comments (48 Responses)
Question 11 (42 Responses)
Question 11 Comments (48 Responses)
Question 12 (43 Responses)
Question 12 Comments (48 Responses)
Question 13 (43 Responses)
Question 13 Comments (48 Responses)

	Group
	The Detroit Edison Company
	Kent Kujala
	The Detroit Edison Company
	Yes
	Yes
	No
	The language "except in specified circumstances such as emergency." introduces ambiguity into this requirement. What would other circumstances be? Is each Responsible Entity allowed to define this on their own? Paragraph 443 of FERC order 706 directs the SDT to provide guidance on defining emergencies. "The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. We also direct the ERO to identify the parameters of such exceptional

	circumstances through the Reliability Standards development process."
	Yes
	No
	CIP-006-2 R1.4 references "physical access controls as described in Requirement R3". R1.4 should reference Requirement R4 since the requirements were renumbered and Physical Access Controls is now R4. CIP-006-2 Introduction, 3. Purpose, it should read something like, ". . . . . to ensure the implementation and continued maintenance of a physical . . . . . " This program is not only being implemented, but will also be maintained going forward. (i.e. – does not make sense to implement a program and do nothing else) CIP-006-2 Introduction, 4.2 The following are exempt from Standard CIP-006-2, in addition to listing the exemptions to NERC Standard CIP-006, they may also want to comment on potentially overlapping security requirements for facilities which are also regulated under the Maritime Transportation Security Act (33 CFR 101/105) and the Chemical Facility Anti-Terrorism Standards. (6 CFR 27) CIP-006-2 R2 Protection of Physical Access Control Systems, sub-requirements R2.1 & R2.2. R2.1 is ambiguous in that it states, "Be protected from unauthorized physical access," yet it does not explain how this is to be accomplished. R2.2 defines the protective measures to be utilized – R4 and R5, Physical Access Controls and Monitoring Physical Access. It appears they want to grant the responsible entity flexibility in R2.1, but then it is limited by R2.2. These two sub-requirements should be combined into one to avoid confusion.
	Yes
	No
	The addition of "and implement the plan in response to Cyber Security Incidents." is awkward. This literally states that the plan will only be implemented upon a security incident, but the plan must be implemented in order to "characterize and classify" reportable Cyber Security Incidents. It might be clearer if written as " The Responsible Entity shall develop, implement and maintain a Cyber Security Incident Response Plan....and execute the plan in the event of a Cyber Security Incident." Remove the "Process for…." language in CIP-008-2 R1.4, R1.5, and R1.6 to be consistent with the language changes in CIP-006 R1.7 and R1.8. Suggested language is as follows: R1.4. Update of the Cyber Security Incident response plan within thirty calendar days of any changes. R1.5. Annual review of the Cyber Security Incident response plan. R1.6. Annual testing of the Cyber Security Incident response plan. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.
	Yes
	No
	Does this mean that the current quarter must end, and then you start counting to the first day of the following 3 quarters, or do you include the current quarter in counting? Why not simplify things and use a number of days, such as: "120 calendar days after applicable regulatory approvals have been received . . . . . ."
	Yes
	No
	Table 2 does not address CIP-006-2 R7 and R8. They should both be 24 for category 1 and 12 for category 2. Table 2 CIP-008-2 R2 category 2 should be changed from 0 to 6 which matches the timetable associated with R1. The 0 implies that a Responsible Entity needs to retain documents relating to requirement, R1.1, which that entity is not yet required to be compliant. Table 2 CIP-009-2 R2 and R3 category 2 should be changed from 0 to 12. Similarly to the comment around CIP-008-2 R2, a Responsible Entity cannot be compliant with exercising a plan that is not required to exist. Changing the timetable to 12 ensures the recovery plan is initially executed in the annual time frame required by R2.
	Yes
	Yes

Group
PacifiCorp
Paul Golden
Compliance Project Management Office (C-PMO)
Yes
No
Suggested modification to R2.3 "Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions assigned to the senior manager to a named delegate or delegates."
Yes
No
Yes to the second bullet. No to the first bullet and other points. R1.1 - It is unclear what is meant by “externally connected”. Does “connectivity” refer to logical or physical connectivity? Is “external” a reference to the ESP in question, or to the entity? Is it a reference to layer 3 (and above)? PacifiCorp recommends some clarifying language similar to the following: •Any device accessible via routable protocol (layer 3) from outside the ESP is an access point unless such traffic is already passing through and controlled (layer 3) by another CIP005 compliant access point. •Additionally, any device serving as an endpoint of an encrypted and/or encapsulated layer 3 (and above) tunnel (IPSEC, GRE, SSL-VPN, SSH, CIPE, etc..) which provides remote network connectivity to the ESP network and not merely application access to the host itself, and where the other endpoint is outside the ESP, is also an access point.” •Externally connected also includes devices accessible via modem or any form of wireless access point providing network connectivity to other devices within the ESP. •Externally connected does not include encrypted communication links where the end points are within the ESP. R1.3 - This should be eliminated. By definition, communication links between discrete ESPs are “out of scope” (CIP-005-2 4.2.2) Additionally, where such links are using routable protocols, the termination point would be a “communication end point” and thus covered by R1.1. This section provides no additional value. R1.5 references to CIP005.R2 and CIP005.R3 should be removed as these are not applicable to the access control and monitoring equipment which are not "Access points". Additionally, the proper security practices for these devices are covered under CIP007 R2-R9. R1.5 (continued) - The access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as mobile devices. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. PacifiCorp believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting mobile devices used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4. PAC proposes the following language: R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for mobile devices, for which the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.
No
No for the third bullet (R3) (See comment on CIP-005-2). Yes for remaining bullets.
No
Other comment: R5.3 - Instead of prescribing specific password construction standards, it would be better to express desired outcomes in terms of measurable entropy. The standards should require a certain level of protection against password guessing and brute force "hash cracking" attacks, but leave specifics to the implementers. For example, the standard could simply require 24 bits min-entropy per NIST Special Publication 800-63.
Yes
Yes
No

	This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule found in Table 3. PacifiCorp has been working toward compliance with the standards under the premise that the generation owner has until December 31, 2009, to become compliant with version 1 standards. For significant changes proposed in version 2, the generation owner will need time to address and comply.
	Yes
	Yes
	Yes
	No
	The new affective date goes above the requirements listed in order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
	Group
	FirstEnergy Corp
	Doug Hohlbaugh
	FirstEnergy Corp
	Yes
	Yes
	No
	Regarding R2.1 and R3, we believe that the phrase "specified circumstances such as an emergency" is ambiguous. It is not clear what would constitute acceptable "specified circumstances" other than an emergency situation. This phrase should be replaced with simply "emergency situations", which would also be consistant with language in other CIP requirements such as in CIP-003 R1.1.
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	No
	While we do agree with the overall objective the team is trying to achieve, we do not agree as presently written and offer the following comments: a) The description of Category 1 seems to imply that a Responsible Entity who has a CIP CA and CCA methodology, but did not identify any CCA assets may be given additional time to comply with the CIP standards when they have identified any CCAs on subsequent annual reviews. However, what is not clear is what triggered the new CCA being identified? The Category 1 description should be clear that it does not apply simply based on "error and ommission" if the Responsible Entity's methodologies for CA and CCA identification have not changed and the Responsible Entity simply overlooked an asset that should have been previously identified and protected. If these

newly identified assets were in service during their initial CIP asset determination, then the entity was not compliant with their initial asset identification and it should be expected that the entity would file a Self Report and Mitigation Plan to obtain compliance. b) FE believes our above comment on Category 1 also applies to the Category 2 description as it indicates in the second paragraph that it refers to newly identified CCA assets but they are not associated with an addition or modification through construction, upgrade or replacement. Again, if the methodologies have not changed, if there was no merger or acquisition, then what triggered the newly identified existing asset? It should be clear that "error and ommission" do not apply. c) We agree with the provisions described for newly aquired assets through mergers and acquisitions when companies may have had differing methodologies. d) We agree with item 3 regarding "Compliant upon Commissioning" for newly planned upgrades that result in new CA and CCA items. e) In general we found the information to be overly wordy and confusing to understand. We suggest the team attempt to greatly consolidate the information. f) Tables 2 should be adjusted such that it can be read and viewed stand alone to the extent possible from the remaining supporting text. For example, Table 2 has no indication that the numbers refer to "months".
Yes
We agree with the Implementation Plan times described for Category 1 and Category 2, however, we believe clarrification is need as to when these provisions apply. See our comments in Question 10.
No
The stand alone document is sufficient and could be easiliy added as a reference document to each standard.
Yes
For the most part we agree with the improvements except for our previous comments in questions 3, 10 and 11. Also, we offer the following additional suggested improvements: CIP-002-2 R3 - The phrase "automatic generation control" should be capitalized since it is a NERC defined term. CIP-003 M1 - The SDT should consider removing the second sentence "Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2" since the language in the first sentence already covers the necessary measure. CIP-005 R2.4 - The word "strong" should be removed since it is not clearly defined and measurable. CIP-007 - R2,R3,R5 - The word "establish" should be removed consistant with the other CIP standards. All that should be required is to "implement and document". - R5.1.2 - Replace "establish" with "have". - R7 - Replace "establish" with "document. CIP-009 - The first sentence in "Sec.B Requirements" which states "The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:" is not necessary and should be removed consistant with the other CIP revisions. FAQ Document - Is the SDT considering changes to the FAQ document to align with these proposed changed to the standards? Or is the FAQ document not a "living" document and was only to be used for the version 1 standards development? Regarding measures in CIP-002 through CIP-009, the drafting team should consider revising the measures to include some guidance on the types of evidence or documentation that a responsible entity should and/or could have to demonstrate compliance. Throughout the standards the phrases "at least" and "at a minimum" are used and we fee that they are unnecessary. It is already understood that the standard requirements are the minimum expectations. Throughout the standards we suggest the SDT add the VRFs for each main requirement. Lastly, it would be appreciated if the SDT would use underlining in addition to the blue colored text to reflect inserted text for readability of black-n-white printed/copied material.
Group
MidAmerican Energy Company
Ray Andrews
MidAmerican Energy, CIP Administration
Yes
No
Suggest an addition: The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
Yes

	No
	Comment: On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. MidAmerican believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4. MEC proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.
	No
	See comment for question 5
	No
	Comment: MidAmerican does not agree with the change within the Purpose section of the standard to change the term “non-critical” to “other.” MEC proposes the following language Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
	Yes
	Yes
	No
	Comment: This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule. MidAmerican Energy Company has been working toward compliance with the standards under the premise that the generation owner has till December 31, 2009, to become compliant with version 1 standards. For significant changes proposed in version 2, the generation owner will need time to address and comply. For applicable regulatory approvals received between January 1 and March 31, revised standards will be effective the following January 1. MEC proposes the following language: Effective Date: The first day of the calendar quarter after at least nine months following the applicable regulatory approvals have been received, as illustrated in the following table. Applicable regulatory approval received - Effective the following Jan. 1- Mar. 31 Jan. 1 Apr. 1- June 30 Apr.1 July 1- Sept. 30 July 1 Oct. 1- Dec. 31 Oct. 1
	Yes
	Yes
	Yes
	No
	The new effective date goes above the requirements listed in order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
	Individual
	Michael Puscas
	The United Illuminating Company
	Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Notheast Power Coordinating Council
Guy Zito
NPCC
No
We recommend that CIP-002 be updated by moving CIP-003 R2 into CIP-002. By moving CIP-003 R2 into CIP-002 all the Requirements that all Entities must complete are in one Standard. The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into the CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone.
No
1 - We recommend moving CIP-003 R2 into the CIP-002 Standard. 2 - We request clarification of CIP-003 R2.3 "the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) and b) the delegation.
Yes
No
"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.
No
1 - We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points". 2 - We request a correction to R1.4 which references R3. We believe this is now R4. 3 - Regarding R1.6, we are concerned with the new word "continuous",

	and that it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4 - We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the entity's change process for any".
	No
	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the entity's change process."
	No
	1 - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2 - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the entity's change process". 3 - Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
	No
	1 - We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed." to "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of completion of the entity's change process." 2 - "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate.
	No
	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)". In addition, Canadian members of NPCC have concerns regarding the standards becoming effective at different dates in different jurisdictions. Coordination is required among government authorities to ensure that standards become effective at the same time in all jurisdictions. 2 - Request confirmation that these Effective Dates apply to these updates (Version 2). 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary, the new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - Clarification required for "the last audit records" and "subsequent audit records" in Data Retention 1.4.2. This comment applies to CIP-002 - CIP-009.
	No
	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entites. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that the CIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some refer to Version 2 (Table 2), and the Requirements do not match CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon Commissioning) Critical Cyber Assets. 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence. 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Asset in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial communications and the new Asset uses IP communications. We

	suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of:"to "c) Planned addition of:". 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
	No
	1 - We recommend that Table 2 clarify the units as months, per page 1. 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
	Yes
	Yes
	We agree with the removal of "reasonable business judgment" and "acceptance of risk".
	Individual
	Steven Dougherty
	Deloitte& Touche, LLP
	Yes
	Yes
	Yes
	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal training and awareness program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
	Yes
	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal dial-up security program and procedure that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
	Yes
	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal physical security program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
	Yes
	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal security management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
	Yes
	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal incident management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
	Yes
	Yes
	Yes
	Will the drafting team include situations that occur through merger and acquisition(M&A)?
	Yes

Yes
Yes
Group
WECC Relibaility Coordination
Linda Perez
WECC Reliability Coordination
Yes
Yes
No
do not agree with with R1.2 that personnel need to be trained before they are granted access. Traning in this area is extensive and we feel the 90 day window allows appropriate training to take place along with our employee orientation.
Yes
Yes
No
R2.3, R3.2 and R4.1 removes an organizations ability to accept minimal risk which cannot be compensated for. R9, we think 90 days is a resaonable time frame, 30 days is too restrictive.
No
no we feel that 90 days is a reasonable time frame.
No
no we feel 90 days is a reasonable time frame.
Yes
Yes
Yes
Yes
Yes
Individual
Chris Scanlon
Exelon
Yes
Yes
Yes

Yes
We support all comments noted for CIP005 in this section with the recommendation to move the word implement before maintain in R2.3 so the sentence reads 'implement and maintain.' Reason for the recommendation is a control must be implemented before it can be maintained
Yes
Recommendation to increase the timeframe in R1.7 to update the physical security plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation. We support all the other comments noted for CIP006 in this section with the recommendation to move the word implement before maintain in R1 so the sentence reads 'create, implement and maintain.' Reason for the recommendation is a control must be implemented before it can be maintained. .
No
Recommendation to increase the timeframe in R9 to document changes to systems or controls to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.
No
Recommendation to increase the timeframe in R1.4 to document changes to the cyber security incident response plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.
No
Recommendation to increase the timeframe in R3 to require updates to be communicated within 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management activity.
Yes
Yes
The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
No
The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
Yes
Yes
Individual
Mark Ringhausen
Old Dominion Electric Cooperative
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
I agree with including this information in the standards so everyone,user and Region, understands what is required. Leaving it in a stand alone document might allow for FERC to unilaterally change the implementation timeframe without stakeholder input. I hate to have to revise the CIP standards again, but this is important.
Yes
Individual
Alan Gale
City of Tallahassee (TAL)
Yes
While I agree with the R4 revision, I disagreee with the removal of the "reasonable business judgement" in all the standards. While this was in response to FERC directive, it creates a one-size-fits-all approach. Every system is different, as is their Risk Assesment Procedure. This will be one of the more contentious issues. While it may be outside the perview of the SDT, the industry has not been given the information that is needed to specifically address the Auroura fiasco. All we know is someone set up a generator and "hacked" in to change the set frequency and damage ensued. We are not aware of what software was in place to protect this "asset" or what controlling software was. Can the specifics of who set up the test and the hardware/software/control systems being utilized be shared with the industry through a NERC Alert Industry Advisory? While I do not think I have my head buried in the sand about the potential for Cyber attack, I do have a problem with taking all-encompassing action with so little information on what caused the initial knee-jerk reaction. The cost of safeguarding a system against such unknown attacks, to a level that will be acceptable during an audit (a second unknown) will surely be a significant burden to many utilities. While entities have some latitude in our "methodology" in identifying Critical Assets, the fact will remain that you have to spend money on new tools and hardware to comply with the existing requirements outside of routine budget cycles at a significant impact to operations. According to the letter from Rick Sergel to the BOT of July 7, 2008 even after we spend a ton of money, we are still susceptible to attack. Without the flexibility of determining cost vs. benefit, we will overachieve the goal of ".. . reasonably ensure the reliability of the BPS. . ."
Yes
Although the "acceptance of risk" ties in with the discusson above on business judgement.
Yes
Yes
Yes
Yes
Although the "acceptance of risk" ties in with the discusson above on business judgement.

Yes
Yes
Yes
It is confusing though.
Yes
Although it can be confusing also.
Yes
Yes
I am for eliminating stand alone documents, althogh this incorporation can be made in Version 3, since you have stated one will be done for the more contentious issues.
Yes
I may not agree with all changes but they do address the FERC Order directives, even though by making these directives, they violate the ANSI approved process that they have stated NERC is required to follow.
Individual
Brian Martin
BC Transmission Corporation
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual

Joe Weiss
Applied Control Solutions, LLC
No
Need to include the NIST Framework in addition to senior management approval
Yes
No
Training needs to be specifically control system cyber security training
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
NIST Framework needs to be addressed NOW!
Group
Southern Company
Marc M. Butts
Southern Company Services
Yes
CIP-002 Section D – Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-002 Section D – Compliance: 1.4.1 – Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-002 Section D – Compliance: 1.4.2 – Should have a time limit to reduce the overall liability of confidential information.
Yes
CIP-003 Section D – Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-003 Section D – Compliance: 1.4.1 – Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-003 Section D – Compliance: 1.4.2 – Should have a time limit to reduce the overall liability of confidential information.
Yes
CIP-004 Section D – Compliance: 1.1.1 does not specify who is responsible for the

	enforcement authority. CIP-004 Section D – Compliance: 1.4.2 – Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-004 Section D – Compliance: 1.4.3 – Should have a time limit to reduce the overall liability of confidential information.
	Yes
	CIP-005 Section D – Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-005 Section D – Compliance: 1.4.1 – Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-005 Section D – Compliance: 1.4.3 – Should have a time limit to reduce the overall liability of confidential information.
	Yes
	CIP-006 R1.1 – Change to the last sentence should be clarifed that it applies to Critical Cyber Assets and not Critical Assets. R1.4 makes reference to "Requirement 3", but the correct reference in the new standard should now be "Requirement 5". CIP-006 Section D – Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-006 Section D – Compliance: 1.4.1 – Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-006 Section D – Compliance: 1.4.3 – Should have a time limit to reduce the overall liability of confidential information.
	Yes
	CIP-007 Section D – Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-007 Section D – Compliance: 1.4.1 – Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-007 Section D – Compliance: 1.4.3 – Should have a time limit to reduce the overall liability of confidential information.
	Yes
	CIP-008 Section D – Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-008 Section D – Compliance: 1.4.1 – Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-008 Section D – Compliance: 1.4.2 – Should have a time limit to reduce the overall liability of confidential information.
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Group
	Luminant Power
	Rick Terrill
	Generation Compliance
	Yes
	Yes

	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	No
	Luminant thanks the Standards Drafting Team for their work addressing improvements to the NERC CIP Standards CIP-002 through CIP-009. As indicated by our "yes" responses to the comment form, in general Luminant agrees with the drafting team regarding the phased approach, implementation plan and the changes to address the time-sensitive issues from the FERC Order. However, on each standard the drafting team changed the language under the Data Retention sections 1.4.1 and 1.4.2. Luminant agrees with the intent of the changes but does not believe the language provides sufficient clarity. Luminant respectfully submits the following suggested language for the aforementioned data retention sections on each standard. 1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002- 2 for the current calendar year and the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation. The Responsible Entity shall keep documentation required by the Compliance Enforcement Authority for an investigation for one year after Compliance Enforecement Authority notice to the Responsible Entity that the investigation is completed. 1.4.2 The Compliance Enforcement Authority and the Responsible Entity shall each retain all requested and submitted audit records from the most recent audit.
	Individual
	Glen Hattrup
	Kansas City Power & Light
	Yes
	No
	In 003 R2, internal political difficulties are created by requiring the designated senior manager to have the authority to implement the security program. Many medium to large utilities have IT departments separate from their operations or compliance departments. In order to find a manager of sufficient direct line authority, you have moved to a level within the organization where the manager will either not have the appropriate level of knowledge to review compliance actions or will not have sufficient time to dedicate to the task. Either way, all that will occur will be a perfunctory signature on the compliance documentation which defeats multiple goals of the program. I believe most utilities will want to comply with the spirit of this provision, but the proposed phrasing will make doing so more difficult.
	Yes

	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	This seems like the most logical place to put those requirements. Otherwise we'll end up with Standards that have to be cross-referenced against multiple sets of documents.
	No
	One change that is particularly troubling is the removal of the "reasonable business judgment" clause on the standards. Without better guidance on what is truly required for an implementation, this leaves the utilities exposed to being found non-compliant despite having done due diligence upon their part. Without some sort of exception or appeals process, utilities are potentially liable for exorbitant costs in order to "secure" their systems to the subjective standard of the auditor. This financial liability could be an excessive burden that will affect their operational ability.
	Group
	Encari
	Matthew E. Luallen
	Encari
	No
	R4 should also include a direct reference to CIP-003-2 R2 to ensure that the Responsible Entities are aware are all applicable requirements. A Responsible Entity that identifies a null CA list must still perform CIP-003-1 R2. This would allow the exemption in CIP-003-2 (4.2.3) to be removed. --General Comment Provided in All Submissions-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	Also see comments on Question 1 pertaining to exemption 4.2.3 --General Comments Provided in All Submissions-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	The new language within R2.1 allows for an exception in specific circumstances. What are specified circumstances? And, if these specific circumstances occur do the individuals ever

	have to take the training? - the prior requirement was within ninety calendar days. An additional crossover requirement exists leading to confusion. CIP-006-2 R3 now states cyber assets residing in a PSP; however the language now in CIP-004-2 does not require access to Cyber Assets to undergo training, awareness and PRAs. We recommend providing further clarification around this requirement. --General Comments Pertaining to All Standards-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	It is very important to define monitoring in the new context. Originally the cyber assets had to be used for the dual purpose of access control and monitoring. Now, simply a monitoring device is considered a cyber asset under this new language. We ask for an additional clarification around to what extent monitoring is covered, for example: 1. The original monitoring cyber asset (device a) 2. The cyber asset receiving alerts from the original device (device b) 3. The cyber asset forwarding the alerts (device c) 4. The cyber asset receiving the alerts (device d) The current language could be interpreted in a way that a blackberry receiving alerts is "monitoring" the ESP. --General Comments Pertaining to All Standards-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	1. The redlining appears to be inaccurate. For example R2 in CIP-006-1 is now R4 in CIP-006-2. This modification is very important to note as compliance monitoring systems may have been defined to key on the requirement field. 2. CIP-006-2 R4/R5/R6 now use bullets instead of numbered identifiers for the individual physical access methods. A unique identifier should be selected to identify these bulleted items. 3. R3 requires cyber assets used in the access control and/or monitoring of the ESP to be in a PSP. Please see our comments in Question 4 (CIP-005-2) pertaining to the extent of what assets need to be in a PSP (device a / b / c / d). --General Comments Pertaining to All Standards-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	1. We recommend striking the following language from the Purpose section - "those systems determined to be Critical Cyber Asset, as well as the other". --General Comments Pertaining to All Standards-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	1. We are confused about the necessity to call out a specific "Cyber Security Incident" response team. Does this no longer require an entity to have a physical security incident response team? --General Comments Pertaining to All Standards-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	--General Comments Pertaining to All Standards-- Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
	No
	This effective date is still open-ended as the process is not complete. Once additional

	comment periods have completed and the revisions have been refined we will provide comment as to the acceptability of this timeframe and the continued assurances of the reliability of the Bulk Electric System. We recommend that the standards become agreed upon and complete and then an effective implementation date be identified. This will provide proper assurances from asset owners that they can indeed meet the timeframe identified while continuing to assure the reliability of the BES. We also are confused regarding the term "calendar quarter" versus a concept of "fiscal quarter". Please provide a clarification.
	No
	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period.
	No
	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period. For instance, the current document details "existing" within CIP-003-2; however - newly identified CCAs may not immediately be able to compliant at zero day with CIP-003-2 requirements. For example R4 requires the information associated with the CCA to be protected. This information may still reside in a non-protected format prior to becoming a CCA - however the implementation timeframe is "existing".
	No
	We agree that the requirement to identify new CCA should be included; however, we believe that a continued need to guide Responsible Entities in the selection of CAs and CCAs is still necessary as separate documents.
	No
	FERC provided directives on nearly all of the current requirements and guidance to include further requirements. The identification of what to modify in a time-sensitive manner was not open for public comment. We recognize the need to act swiftly to protect the assets; however, assurances also need to be made to protect system reliability. As an example, we feel that further clarifications around how to select critical assets and critical cyber assets would have provided a greater impact on the process and recommend that a public comment period be opened for the current draft guidelines. Therefore we recommend providing public comment periods to help the selection process of which FERC directives to introduce in the next phase of changes.
	Group
	TransAlta Centralia Generation, LLC
	Mark Phillips
	Joanna Luong-Tran
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes

Yes
Yes
Yes
Yes
Individual
Martin Bauer
US Bureau of Reclamation
No
The modification of the standard to require that a specific individual approve the risk-assessment methodology appears to be overstepping the bounds of the authority of the regulatory agencies as it pertains to improved reliability. It is difficult to imagine or prove that having one individual within an agency approve a methodology (as opposed to making the entity responsible for having and using a methodology) improves system reliability. Such a requirement is also not consistent with most of the other BES reliability standards. For consistency, the standard should refer to "Responsible Entity" rather than specific individuals within the organization. That determination is the sole discretion of the Responsible Entity and was not required by FERC. FERC required, in paragraph 236, that "internal, management, approval of the riskbased assessment" is required. FERC further clarified: "A responsible entity, however, remains responsible to identify the critical assets on its system". To that end the standard should require that the 'Responsible Entity" ensure that management has approved the risk based assessment. The "Responsible Entity" is then responsible to demonstrate that the requirement has been met and who approved it.
No
The reference to a senior manager in paragraph 381 was not intended be a requirement. FERC did allow registered entities some flexibility, to wit: "The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve". The modification by the SDT, which specifies delegation by the "senior manager", is intrusive upon the Responsible Entity's organizational structure. It is sufficient to require that the Responsible Entity must be able to produce documentation of who has responsibility for the CIP implementation. For geographically diverse organizations, that responsibility will change depending on the location of the affected systems. Each Responsible Entity generally has identified an individual who is authorized to submit documentation in response to a Regional Entity's requests or through the certification process. The specific requirement that the senior manager have the authority of leading and managing CIP is not the same as requiring certification and may not fit with the organizational lines of the Responsible Entity. Organizational structures must not be legislated in industry standards, especially when the organizations have a vast array of responsibilities and authorities that govern their funciton. Reclamation has functional responsibilities delegated to Regional Directors in order to manage the vast array of legislated mandates. To require Reclamation to alter its organizational structure in no way improves the reliability of the BES and the requirement appears arbitratry. Each entity certifies that it complies with the integrity of its security through one individual who is authorized to speak for the agency. The requirements should focus on the desired performance outcome which is needed to maintain reliability of the power system, not how the performance is accomplished.
No
Requirement R2 needs to more specifically distinguish between access types and required training. Individuals with physical access may only need general security awareness training, whereas those with physical and logical access may require specific role-based training. The requirement, as written, addresses proper use of cyber assets, physical and logical access controls, proper handling of information, etc., in what appears to be an all-inclusive manner. Some of these training requirements would appear to be unnecessary for an individual who may only need limited physical access and the requirement should support this. The requirement does not recognize that Entities may have a more rigorous background check process which takes longer than the abreviated process described in the standard. While

	describing the minimum helps to clarify what is needed, the standard should allow Entities that have more rigurous requirements longer time frames to implement the background checks. In most cases the bakcground checks timeframes are not within the control of the Entity. In addition the standard would hamper the ability of existing experienced staff who have passed a more exhaustive check from operating thereby defeating the value to reliability. Can the requirement, R3, be structured in such a manner as to support access following initial screening in situations where full investigations may take a significant period of time? As an example, a national security check resulting in a clearance may take an extended period of time, limiting an organization's ability to utilize an employee - even in a decreased sensitivity role - while awaiting results. If the employee is allowed access - even limited - following a preliminary check (through local/national law enforcement agencies), would this meet the intent of the requirements while awaiting the results of a full and more comprehensive investigation? Further, is there a means, within the present requirements, to address the temporary "grandfathering" of individuals who have access today while they are undergoing investigations? Without such an allowance, staff availability, during investigation activities, could be severely limited.
	No
	The standard should be worded to be applicable for existing dial-up access or if dial-up access is added.
	No
	The requirement that the Physical Security plan be approved by a single senior manager is not appropriate. It should be sufficient to require that the entity have a management approved plan. As stated before, submissions from the regional entities in geographically diverse entities pass through and are certified by the entity's complaince POC and represent an official entity position and commitment to action. To require more adds an unecessary organizational and administrative burden.
	No
	More rational is needed to expain the decision to remove "acceptance of risk" and "reasonable business judgement" language from CIP requirements while leaving the ability to identify "exceptions" through cyber security policy (CIP-003-2, R3.) With this exception in place, entities will be able to establish "policy" that will allow for deviation from the requirements outlined in the Standards. If the intent of the changes was to limit implementation disparity across all entities by removing "risk based decisions", the potential remains that an entity will establish exceptions through relaxed "policy" and the disparity will remain. If the intent was to remove any avenue for not meeting or implementing the requirements, entities may continue to accept "risk based decisions" (although not formally identified as such) by pursuing relaxed policy via exceptions (CIP-003-2 R3). Further, entities may have numerous "systems" of differing capabilities and generations. To require that exceptions be documented in "policy" does not acknowledge the diversity of systems that may be in service in an organization in as effective a manner as documenting exceptions as a function of the system, its environment, and its criticality. Such documentation would be better addressed through specific risk-acceptance decisions tied to specific systems, rather than to an all-encompassing "policy." Finally, as CIP-003 is amended, entities may not implement or meet certain requirements, as long as, they are identified and documented as "policy exceptions." Was this the intent of the authors? We recommend that risk-managed approaches to cyber security requirements be reinstated into the requirements, recognizing that such a change will require FERC to reassess their order.
	Yes
	Yes
	Yes
	Yes
	No
	The agreement would be based on the response to the CIP-004 background check requirement timeframe. The milestones would require adjustment for more exhaustive background checks.
	No
	Inserting the information and time lines for newly identified Critical Cyber Assets and newly

registered entity information into the body of the standards will cause unnecessary confusion regarding the implementation of the standards. By retaining the current stand-alone implementation plan it provides a ready reference and single point of information for all new Critical Cyber Assets and newly registered entities.
No
The revisions are moving these standards away from "Critical Infrastructure Protection" towards "Cyber Infrastructure Protection." We believe this move strays from the original intent of Critical Infrastructure Protection as defined by the initial requirements. By focusing solely on the Cyber aspect, many important aspects of critical infrastructure protection will be lost. We reject any efforts to modify CIP from Critical Infrastructure Protection to Cyber Infrastructure Protection.
Individual
Edward Bedder
Orange and Rockland Utilities Inc.
No
We recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. 1 - The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. 2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall …
No
1 - We recommend moving CIP-003 R2 into the CIP-002 Standard. 2 - We request clarification of CIP-003 R2.3 "the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the delegation (i.e. does it have to explicitly reference the standard and requirement?)
No
CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
No
"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
No
1 - We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2 - We request a correction to R1.4 which references R3. We believe this is now R4. 3 - Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4 - We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"
No
We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
No
1 - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop. maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2 - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within within thirty calendar days of completion of the Entity's Change Process" 3 - The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4 -

	Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
	No
	1 - We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed." to "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of completion of the Entity's change process." 2 - "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
	No
	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009
	No
	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entites. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan is applies to Version 2 because some references Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of:"to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
	No
	1 - We recommend that Table 2 clarifies the units as months, per page 1 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
	Yes
	Yes
	Individual
	Martin Narendorf

CenterPoint Energy
No
An additional modification that was proposed by the SDT in R1.7 reduced the amount of time allowed for making changes and updates to the physical security plan from 90 days to 30 days. CenterPoint Energy strongly disagrees with this change. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any physical security plan changes.
No
CenterPoint Energy strongly disagrees with the proposed modification in R1.4 reducing the amount of time allowed for making changes and updates to the Cyber Security Incident Response Plan from 90 days to 30 days. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any changes.
No
Regarding R3, CenterPoint Energy acknowledges that updates to a recovery plan and communication of those updates should be completed in a timely manner; however, CenterPoint Energy believes the SDT went too far in reducing the timeframe for communicating updates from 90 days to 30 days. CenterPoint Energy believes that 30 days is too constraining. Furthermore, in FERC Order 706, paragraph 731, the Commission separated the time allowed for updating recovery plans (30 days) and the time allowed for communicating those updates (90 days), and was willing to consider timeframes other than 30 days. CenterPoint Energy proposes a 60 day window for updating a recovery plan and retaining the 90 day window for communicating the updates to responsible personnel. This would allow adequate time for the appropriate documentation changes to be made and is still timely for communicating to personnel.
No
See responses above to Q5, Q7, and Q8. In addition, the SDT changed the data retention wording in CIP-002 through CIP-009 such that "the Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records." CenterPoint Energy believes the retention time should be more defined and proposes adding "until the next scheduled audit" to make it clear that data retention is on a rolling basis.
Individual
Kris Manchur
Manitoba Hydro
Yes
No
In CIP-003 R2.3 the assignment to delegate authority could be done specifically or by assignment through the entitities policies. It should not be necessary to perform specific delegation for all circumstances which necessitates additional overhead for maintaining such documentation of delegation from the senior manager. The webinar on the revisions to the CIP Standards and other recent discussions mentioned the possible creation of a new process for instances when the phrase "where technically feasible" is applied. These instances might

	also be exceptions to a responsible entity's cyber security policies. Any new process dealing with "where technically feasible" must be supported by additional requirements(s) in the CIP Standards. Responsible Entities should be given direction in the CIPC Standards for identifying, documenting, managing and approving internally these instances. An additional requirement based on CIP-003-1 R3 Exceptions would provide the required direction for industry. Additional requirement(s) must included prior to further industry commenting or balloting on revised CIP Standards or before any new industry process is implemented for "where technically feasible".
	Yes
	Yes
	No
	The wording in R2 should be: "Cyber Assets used in the access control and/or monitoring and/or logging access to the Physical Security Perimeter(s)", to reflect similar wording in R3, and to include other devices or systems used in access control, such as authentication systems.
	Yes
	Yes
	Yes
	Yes
	No
	The new implementation plan needs to clearly state that the categorization is only applied to newly identified Critical Cyber Assets, and not to all Critical Cyber Assets. The new implementation plan should also state that the categorization of a Critical Cyber Asset expires and is no longer required when that Critical Cyber Asset becomes compliant. Table 2 needs to indicate that the milestones listed are in months. The title for Table 3 needs to be revised to indicate that the table is to be used for Registered Entities which have identified their first Critical Cyber Asset (Category 1), and for newly Registered Entities.
	No
	CIP-003-2 R3, R4, and R5: The milestones should be changed to 6 months. Although the information protection, access control and change control and configuration management programs exist, the requirements also include implementation, which will require some time to meet compliance. CIP-008-2 R2: The milestone should be changed to 6 months, the same as R1. The documentation required in R2 is dependent upon the elements in the Cyber Security Incident Response Plan developed in R1. CIP-009-2 R2 and R3: The milestones should be changed to 6 months, the same as R1. The exercises and change control in R2 and R3 are dependent upon the elements in the Recovery Plan developed in R1.
	Yes
	Implementation plans which expire should be stand-alone docuements from the standards. On-going implementation plans should be incorporated into the standards to create self-contained standards.
	Yes
	Individual
	Anita Lee
	Alberta Electric System Operator
	No
	The functional entity (e.g. the Balancing Authority, etc) should be designated as the responsible entity for this requirement, not an individual. This would be consistent with other ERO standards. Also, R1 implies that the purpose of this standard is not only to identify the

	"Critical Cyber Assets" but also the "Critical Assets" (which must be done before you can identify the Critical Cyber Assets), and hence we suggest that either the identification of "critical Assets" be specified in its own and separate standard or the Title and Purpose of CIP-002 be clarified to state that there are 2 purposes to this standard. We suggest that R1 should be re-written to improve clariity. R1, as currently written, contains not only a single requirement, but with at least two, and possibly three or more requirements embedded in it. The accountabilities for these different requirements could be different within an organization, so assigning them to one person would be inappropriate.
	Yes
	However, we would like to comment that the responsibility for meeting requirements in standards must lie with the functional entity, not an individual within the entity. Also, we don't believe details on how delegation is done within an entity should be included in a standard. We propose R4 be revised to: "Annual Approval — The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null).
	No
	The term "specified circumstances" implies that a set of circumstances is specified somewhere. Where is this list and who will decide what comprises it? Suggest that this list be clarified.
	Yes
	Yes
	R1.1 is missing the word, "critical" for Cyber Assets. There is no need to have a requirement for assets that are not critical.
	Yes
	Yes
	Yes
	Individual
	Greg Mason
	Dynegy
	No
	Agree with requiring management approval of the risk-based assessment methodology. Also, suggest moving CIP-003, R2 into CIP-002 so that all the Requirements that all Entities must comply with are in one Standard.
	No
	Agree with proposed modifications except recommend moving CIP-003, R2 into the CIP-002 Standard (see comment on Item #1).
	Yes
	Yes

No
1. Recommend changing R1.2 to require identification of all "physical" access points. 2. Correct R1.4 to reference R4 instead of R3. 3. Eliminate "continuous" from R1.6. This term is not auditable.
Yes
Yes
Yes
Yes
No
Under the Category 2 heading, the proposed method for handling the case of a business merger or acquisition when any of the Responsibe Entities involved had previously identified Critical Cyber Assets is inequitable and inconsistent with the proposed handling of the case when all Registered Entities have identified Critical Cyber Assets. Under the Category 2 heading, in the case of a business merger or acquisition when any of the Responsibe Entities involved had previously identified Critical Cyber Assets, it really only matters if the acquiring or controlling Responsible Entity had previously identified Critical Cyber Assets. If the acquiring or controlling entity had not previously identified any Critical Cyber Assets it will have no CIP Compliance Program and it should be required to meet the same Category 1 (instead of Category 2) milestones established for the case where neither Registered Entity involved in merger had previously identified any critical Cyber Assets. In addition, in the case when all Registered Entities involved in a merger have identified Critical Cyber Assets the merged Responsible Entity is required to meet Category 2 milestones after one calendar year from the merger date. This provision in effect grants the Merged Responsibility Entity in this case the approximate equivalent of having to meet Category 1 milestones. This approach further justifies the revised approach suggested above for the former case.
Yes
Yes
Yes
Group
Bonneville Power Administration
Denise Koehn
Transmission Reliability Program
Yes
Yes
Yes
No
The revision to CIP-005-2 R1.5 references only CIP-006-2 R3. CIP-003 R3 requires that the organization identify the Physical Security Perimeter. In the original CIP-005-1 R1.5, the physical protections had to meet CIP-006-1 R2 and R3 which are now renumbered R4 and R5 in CIP-006-2. This represents a major revision and a much less robust security in the physical protection requirements for cyber assets used for access control or monitoring of the Electronic Security Perimeter. To retain the original intent of CIP-005-1 R1.5, the requirement must include a reference to CIP-006-2 R3, R4, and R5.

No
While the majority of the revisions to R1 do provide clarity, the revision to Requirement R1.1 is less clear than the previous version and represents a change to the requirement. In the previous version, R1.1 requires that the Physical Security Plan address "Processes to ensure and document that" all Cyber Assets within an Electronic Security Perimeter reside within an identified Physical Security Perimeter consisting of a six-wall border. With this new revision, the Physical Security Plan shall address all Cyber Assets within an Electronic Security Perimeter. Address cyber assets how? There is no longer any requirement to describe the process the organization uses to ensure that cyber assets reside within an identified Physical Security Perimeter. Is the intent of this revision to clarify that a Physical Security Plan must simply exist and address identified Physical Security Perimeters protecting Cyber Assets within an Electronic Security Perimeter? There is no requirement for Physical Security Plans for cyber assets used for access control and/or monitoring of Physical Security Perimeters or Electronic Security Perimeters. If the intent of Phase 1 changes to R1 are simply to provide clarity, then recommend retaining the original R1.1 text from the previous version and make changes to R1.1 in a later phase of Project 2008-06 - Cyber Security Order 706.
Yes
Yes
Yes
Yes
Yes
Yes
No
Including the implementation plan information in the individual CIP standards would greatly increase the size and complexity of each standard. All NERC Reliability Standards, including CIP, must be interpreted using various stand-alone documents (e.g., NERC Glossary of Terms Used in the Reliability Standards, NERC Reliability Functional Model, Compliance Monitoring and Enforcement Program, etc.). It's not a problem having the Implementation Plan available as a separate link or as a companion document to the CIP Reliability Standards.
Yes
Individual
Tim Conway
Northern Indiana Public Service Company
No
I do support the recommended change to require management approval of the risk-based assessment methodology per FERC Order 706, paragraph 236. I would like to recommend the addition of some language to CIP-002-2 Req 4. Currently the language in R4 directs the responsible entity to comply with CIP-002-2 R1-R3 and retain a record of the resulting CA and CCA asset list (even if that list is null). My concern is that if the list is null the entity may feel they have completed all necessary actions for compliance. There is however compliance actions for an entity with a null list contained within CIP-003-2. As it stands there is an oddly placed exemption in the applicability section of CIP-003 4.2.3. I would recommend the inclusion of language in CIP-002-2 Req. 4 to identify the need for compliance with CIP-003-2 R2 as well as the currently referenced CIP-002-2 R1-3; in order to contain all applicability for CIP-002-2 R4 in one location and in turn removing the exemption in CIP-003-2. As there is no other means through the use of this comment form I would also like to comment on changes made in CIP-002-2 that repeat throughout CIP-002-2 – CIP-009-2 In the purpose section of CIP-002-2 I would like to see as a component of this draft, an attempt to develop alternative language to replace reasonable business judgment as mentioned in Order 706 in paragraph 135. In the Data Retention section of CIP-002-2 I would like to request clarification on the

	language added to 1.4.2. As the language was there was a limit on data retention that matched the audit enforcement period of three years. The language provided currently removes this limit and extends the retention into perpetuity as well as leaving it unclear which entity is responsible for retaining the data into perpetuity.
	No
	As stated in question 1 I believe the revised applicability in CIP-003-2 section 4.2.3 is oddly placed as an entity could read CIP-002-2 in entirety and feel that the resulting null asset list excludes the entity from any other CIP standards. If a single requirement also applies to an entity that has a resulting null list, I believe it is better to call out the additional requirement within CIP-002-2 R4 rather than adding revised applicability language to CIP-003-2.
	No
	Clarification regarding the definition of specified circumstances and emergency conditions is needed. Additionally, language needs to be added to clarify what steps need to be taken if an emergency occurs and access is granted. As the draft reads, an entity could declare an emergency, grant access, and document the emergency condition. There is no language directing follow up action that would ever require the responsible entity to perform training or a PRA of the individual that was granted access under the emergency condition. Depending on the direction provided from the drafting team in regards to what would consist of an emergency, the removal of the 30-90 day after the fact language may create significant concern in regards to bargaining unit operations and service personnel. Secondly, I have a comment regarding the additional clarifying language that was added to CIP004-2 R1 to indicate applicability to critical cyber assets. I understand that this language was added to provide uniformity in scope between CIP-004-2 R1, R2, and all of the respective sub-requirements. I have a concern regarding the absence of the CCA language in CIP-004-2 R3. I feel R3 should be modified to include similar CCA language to provide uniformity with R1, R2 and the R3 sub-requirements.
	No
	I would request a clarification on scope and depth of the devices to be included in the access control and/or monitoring. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or monitoring of the ESP. I am concerned with the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP.
	No
	In future drafts I would encourage the drafting team to enable track changes on the modifications to the requirements numbers as well as the text. Modifications to requirement numbers, especially in CIP-006-2 were not consistently red-lined to display where the content was formerly referenced in the existing CIP-006-1. Regarding CIP-006-2 R2 I would request a clarification on scope and depth of the cyber assets that authorize and/or log access to the PSP. The previous language would have limited the devices to those that performed control and monitoring of the PSP (traditional physical access control security systems, and localized panels that communicate with the main system). The new language provided in the draft under CIP-006-2 R2 modifies the scope to include cyber assets that authorize and/or log access to the PSP. I am concerned with the depth of devices involved in the authorization or logging chain. Specifically: log correlation servers, backup and recovery servers, camera's, badge printing workstations, camera monitoring stations, log printers, etc.. In the current draft it is unclear whether the device performing the authorization and/or logging is the only cyber asset that is subject to the requirements specified in CIP-006-2 R2.1-R2.2 or if all devices involved in authorization or logging are subject to those requirements specified in CIP-006-2 R2.1-R2.2. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets that authorize and/or log access to the PSP. Regarding CIP-006-2 R3 I reiterate my request for a clarification on scope and depth of the devices to be included in the access control and/or monitoring of the ESP. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or

	monitoring of the ESP. I am concerned with the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP. When providing the scope and depth clarification of these cyber assets, the drafting team needs to give consideration in regards to an entities ability to satisfy the new CIP-006-2 R3 requirements of containing all of the cyber assets used in the access control and/or monitoring within an identified PSP. In regards to CIP-006-2 R4-R6, I believe the sub requirement identifiers were removed as they are not specific requirements, but rather a means to satisfy the requirement. I believe the bullet items need some level of identifier for reference purpose. Potentially a B4.1, B4.2, etc. this would allow for an entity to reference the manner in which they satisfy the requirement.
	No
	Within the purpose section of CIP-007-2 I would recommend the removal of the following language “those systems determined to be Critical Cyber Assets, as well as the non critical.” as this language is redundant.
	No
	In CIP-008-2 R1.2 I would like a clarification of the additional language detailing Cyber Security Incident response team requirements. This additional language implies Cyber Security specific training or a core set of knowledge requirements for the incident responders. What will be the measuring stick to determine if an incident responder is a Cyber Security Incident responder or a non-cyber security incident responder?
	No
	I do not agree with the reduction from 90 to 30 days. I would propose to provide uniformity and match the modified requirement under CIP-007-2 R9, which requires the modifications to be documented within 30 calendar days after completion versus the CIP-009-2 R3 language which requires the updates to be communicated within 30 calendar days after completion.
	No
	I have difficulty responding with acceptance or denial of an implementation schedule when I am not fully aware of what the final draft is going to consist of. Secondly, as this language stands I would like to see a proposed time line based on an example NERC BOT adoption date. I am unclear on weather the version 2 standards would be implemented in parallel with the existing version 1 implementation schedule, in series, or only begin implementation after FERC approval as this draft is occurring due to FERC directed changes. I am also slightly confused on the audit process and which version of various CIP requirements would be applicable as the responsible entities move into an AC status, while the version 2 standards could be BOT approved but not FERC approved.
	No
	Moving through the existing phases, I do not believe the steps provide for a situation in which a utility wishes to improve or strengthen the risk-based methodology. If a utility has an existing CCA and strengthens the methodology process which in turn produces a new CA and in turn new CCA’s, the utility would find itself in immediate non-compliance. Based on this situation and using the flow chart contained within the proposed implementation schedule document, the responsible entity would already have an existing CCA, the Cyber assets of the new resulting CA would already be in service, and it would be a planned change as the utility chose to strengthen the existing methodology. The flow chart result would be compliant upon commissioning, and the cyber asset is already in service, therefore the real world result is immediate non-compliance. I believe this is counter productive as NERC and FERC would encourage an entity to strengthen the risk-based methodology. The current proposed implementation schedule would encourage a utility to not strengthen the risk-based methodology over time in order to remain in compliance. I believe additional provisions need to be made.
	No
	I do not believe CIP-003-2 R3-R6 should be assumed to exist under category 2 assets. An entity may need to identify exceptions, information, provide access control to that information and implement change control procedures on the newly identified asset. I also do not believe that it should be assumed that an entity can obtain the necessary financial capital to implement systems for compliance in any immediate fashion.
	Yes

Yes
Not sure if the question pertains to the CIP draft modifications or the proposed implementation schedule.
Individual
Robert Huffman
CoreTrace
Yes
Yes
Yes
Yes
No
The modifications above are acceptable, however R4.2, as written, implies that all anti-virus and malware prevention tools have signatures, which is not true. Specifically whitelisting or behavioral approaches do not require signature updates. Whitelisting in particular provides greater antivirus/antimalware protection than traditional signature based antivirus, including zero day protection, yet does NOT require “signatures”. Whitelisting relies on a positive security model that complements CIP 003 Configuration Control Requirements. By clarifying that traditional signature based antivirus is not required, NERC opens up the range of platforms and systems that can be protected greatly. For example, traditional antivirus does not exist for most Unix based systems, however whitelisting does. Propose revising R4.2 to read as follows: R4.2. If the Responsible Entity chooses to implement signature based antivirus or malware prevention tools the Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures. This requirement does not apply for non-signature based antivirus or malware prevention tools such as those based on whitelisting or behavioral analysis.
Yes
Yes
Yes
No
To include the distinct procedures for newly identified Critical Cyber Assets would introduce a level of complexity and confusion into the current standard. As they stand today the CIP requirements are easy to understand and useful. A reference to the standalone implementation plan in the CIP body would be useful and sufficient and ensure that the information in the implementation plan was not overlooked.
Group
Consolidated Edison Company of New York, Inc.
John Lim
Consolidated Edison Company of New York, Inc.
No

We agree with the proposed modification, but have suggestions which affect CIP-002 in one area of the Leadership requirement which would be more logical. CIP-002 requires the approval of the Senior Manager for many requirements, and is the standard that determines whether other CIP standards are applicable to the Entity. In order to streamline compliance filing in these cases, and also as a more logical place for the identification of a Senior Manager, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. 1 - The senior manager has not been identified in CIP-002. Many requirements make reference to the Senior Manager or delegate. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. This is the preferred option. Or 2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall …
No
1 - We recommend moving CIP-003 R2 into the CIP-002 Standard. (See comments to Question 1). 2 - We request clarification of CIP-003 R2.3 "the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the requirements for what the delegation must contain (i.e. does it have to explicitly reference the standard and requirement?)
No
CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
No
"Dated" is used only in the Measures (M1, M2, M3, M4, M5). The corresponding requirements do not state a requirement for a date: adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
No
1 - We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2 - We request a correction to R1.4 which references R3. We believe this is now R4. 3 - Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4 - We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any": a change generally includes more processes than just the change, e.g. acceptance period, required internal approvals, "as built" regulatory approvals.
No
We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process." See comments to question 5.
No
1 - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop. maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2 - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within within thirty calendar days of completion of the Entity's Change Process" (see questions 5). 3 - The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4 - Measure M1 is one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
No
1 - We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty

calendar days of the change being completed." to "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of completion of the Entity's change process." 2 - "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
No
1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009
No
1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entites. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some reference Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of:"to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
No
1 - We recommend that Table 2 clarifies the units as months, per page 1 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Yes
Yes
We agree that Phase I addresses the time-sensitive FERC Order directives to remove "reasonable business judgment" and "acceptance of risk".
Individual
Darryl Curtis / Greg Ward
Oncor Electric Delivery LLC
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The timeframes in Table 2 are reasonable. However, CIP-002-1 currently specifies that an asset is not designated as a Critical Asset until the annual application of the Risk-Based Methodology. A cyber asset is not a Critical Cyber Asset unless it is essential to the operation of the Critical Asset. Category 3 "Compliant upon Commissioning" is not a current requirement of CIP-002-1 and represents a significant change to the current standard. This seems to imply that the Risk-Based Methodology must be applied continuously, not just annually. "Compliant upon Commissioning" should only apply to replacing existing Critical Cyber Assets. New Critical Cyber Assets identified by CIP-002-1 Requirement R3 should utilize the timeframes in Category 2
Yes
Yes
Yes
Individual
Bob Thomas
Illinois Municipal Electric Agency
Yes
No
IMEA agrees with the intent of the proposed modifications, but recommends they be incorporated into CIP-002-1 (indstead of CIP-003-1) modifications for clarification of applicability regardless of Critical Cyber Asset identification.

Individual
Cathie Mellerup
Ontario Power Generation
No
Measures M2 and M3 add a requirement by specifying the lists of Critical Assets and Critical Cyber Assets must be dated. M2 references Requirement R2 and M3 references Requirement R3. Neither R2 or R3 require a list to be dated.
No
R1.5 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those which are used to access CCAs
No
Requirement R2.1 will limit the ability of entities to leverage existing personnel to perform such duties as allocating access cards to legitimate visitors. Such duties are frequently delegated to trained reception personnel. OPG believes that allowance must be made for workstations in reception areas and selected offices areas (e.g. Human Resources departments). Cyber controls such as dual authentication on the workstation would be sufficient to meet the protective needs of the system. As noted earlier with respect to CIP 005-2 R1.5, OPG believes that CIP-006-2 R3 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those which are used to access CCAs. With respect to R1.6 there is concern that the addition of the new word "continuous" it will be difficult to demonstrate compliance. Requirements need to be enforceable. We recommend removing "continuous". We are concerned with the change in R1.7 reducing the time to update the Physical Security Plan from 90 to 30 calendar days. In a large organization this timeframe may not be achievable. Changes to CIP-006 R1.1 open up concerns about the protection of non- Critical Cyber Asset components such as cables. To eliminate this concern we request that the wording of the last sentence be returned to read "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets."
No
Reducing the timeframe for documenting changes to systems or controls in R9 from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.
No
Reducing the timeframe to update the Incident Response Plan from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.
No
Reducing the timeframe to communicate updates to CCA recovery plans from within 90 to within 30 calendar days introduces a constraint that may not be achievable in a large organization.
No
We note that the implementation plan for newly identified Critical Cyber Assets specifies that it applies to "CIP-002-1 through CIP-009-1 and their successor standards". We further notice that in Milestone Category 2 an number of requirements have a six (6) month timeframe specfied for compliance. In effect, the identification of a new CCA at an Entity today would be required to be fully compliant with respect to that new newly identified CCA before December

	31st 2009 - the Compliant deadline for all other CCAs.
	No
	We interpret that the plan seems to collapse together the Compliant and Auditably Compliant milestones. We note that it is not possible to identify a new CCA, bring it into a state or Compliant (as defined in the currently applicable standard) and have one year of data and records as required to be Auditably Compliant. We believe clarification is required in this area.
	Individual
	Jim Sorrels
	American Electric Power
	Yes
	Section R4 of the Requirements category does not clearly define what type of unit the senior manager represents. We would suggest a clarifying comment like "for each responsible entity" be added following the word "delegate(s)." This does not appear again in any of the following standards. However, throughout all of these standards, the drafting team has introduced a new term in its use of "Responsible Entity." If this term is to be used, it should probably be considered by the NERC organization with corresponding updates to lists of compliance term glossaries and/or definitions.
	Yes
	Refer to comments provided in questions 1 and 13.
	Yes
	Refer to comments provided in questions 1 and 13.
	Yes
	Refer to comments provided in questions 1 and 13.
	Yes
	Refer to comments provided in questions 1 and 13.
	Yes
	Refer to comments provided in questions 1 and 13.
	Yes
	Refer to comments provided in questions 1 and 13.
	Yes
	Refer to comments provided in questions 1 and 18.
	Yes
	To add further clarity, AEP suggests that the following text be added to the effective date statement above. " . . . after applicable FERC approvals have been received and such approval is posted in the public registry (or the . . . "
	Yes
	Yes
	Yes
	AEP believes that there should be a statement in the standard providing a reference to the implementation plan and that the implementation plan be included in an appendix of the standard.
	Yes
	As described above and following, AEP belives that there are a number of concepts that need to be discussed and clarified in the standards. AEP requests clarication be added about changes to Data Retention item 1.4.2. NERC reference materials suggest that the Compliance Enforcement Authority is solely responsible for keeping the last audit records. AEP does not believe that expanding the role of the Registered Entity, beyond that in any other standard, to include keeping audit documents is necessary or appropriate. However, there may be

	circumstances where confidential underlying data concerning critical infrastructure should only be retained only by the Registered Entity, but, even in such circumstances, auding records should solely be retained under requirement by the Compliance Inforcement Authority. Technical consideration should be given to determining the response to the "Compliance Monitoring Period and Reset Time Frame" section. The drafting team reference guide has suggested time periods aligning with audits cycles and less than monthly reset time frames. The response that it is not applicable does not appear consistent. Lastly, item M1 under Measures has inadvertently dropped the "The" while the remaining M2 - M4 do contain "The" at the beginning of each sentence. In some of the following CIP standards, it is presented correctly, and, in others, it is not aligned within the M1 item.
	Individual
	Dan Rochester
	Ontario IESO
	No
	Standards should hold a functional entity(ies) responsible for meeting the requirements,not a person or a position. Furthermore, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 be revised to: "Annual Approval — The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)" If appointing a senior mangager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.
	No
	With respect to individual bullet points: (1) We find this question confusing. We interpret Applicability as written to mean that those Responsible Entities that have determined that they have no Critical Cyber Assets need only to meet R2 of CIP-003. The question as posted here seems to suggest that R2 of CIP-003 only applies to these Responsible Entities, but NOT to those other Responsible Entities that have identified that they have Critical Cyber Assets. Please clarify. Currently, only CIP-002 is applicable to entities without Critical Assets. Thus, the recommended modification to CIP-003 would be insufficient for accomplishing the intent of the change. One solution might be to move the Senior Manager appointment requirement from CIP-003 R2 to CIP-002 (as suggested under Q1), or incorporate the requirement for a Senior Manager appointment by reference within CIP-002. (2) Agreed, and this is consistent with our comments on CIP-002, above. (3) Agreed (4) Agreed (5) Agreed
	Yes
	Yes
	No
	With respect to individual bullet points: (i) R1: The reference to the Senior Manager should also refer to CIP-003 R2 to clarify the requirement. (ii) CIP-006 R1.6 should not require "continuous" escorted access, since demonstrating compliance with such requirement would be impossible. As an alternative, wording might indicate that visitors are to be escorted in a manner that ensures their actions can be supervised and unauthorized disclosures prevented, and/or only authorized employees can be escorts. (iii) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" (iv) R1.4, reference to R3 should read R4.
	Yes
	No
	The new sentence in R1.6 is not a requirement and does not add any value; in fact, it may create confusion - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence.
	Yes

Yes
Yes
We believe the proposed implementation plan is reasonable and appropriate.
Yes
We believe the proposed implementation plan is reasonable and appropriate.
No
We believe that an implementation plan managed as a separate document is a more logical choice. Information is less likely to be repetitive and other standards can reference it as necessary. However, where an issue pertains to a single standard, it would be appropriate to include the pertinent implementation information within that standard.
Yes
Individual
Kirit Shah
Ameren
Yes
None.
Yes
None.
No
The elimination of the 30 day temporary access time will have a significant “operational” impact to fill personnel positions in a timely manner within protected areas. Without the 30 day temporary access criteria, personnel will not be allowed “unescorted” access into a facility until the candidate has completed training and a background check is completed, reviewed and returned with a positive and acceptable response. Additionally, mandating that another employee watch or “escort” the new candidate all the time during their shift is both a nuisance and a possible safety hazard. It is important to note that this proposed change is a “180 degree conceptual change” from what was a noticeable and unwavering stance that most companies took when the original CIP standards were implemented. Not being able to shift personnel around from one area of the company to the protected-area assignments (when personnel are re-assigned) immediately, places an unnecessary burden on both areas of the company. When comparing the proposed change to the current process, the benefits gained by the elimination of the 30-day temporary access window clearly don’t outweigh what is already a solid and workable solution.
Yes
Yes
No
Acceptance of risk for certain ports and services is within security best practices. Mitigating controls for certain ports and services could effect the reliable operation of the bulk electric system.
Yes
Yes
Yes
Yes

Would like to see a clarification on what is intended by phrase "planned change".
Yes
Yes
Yes
Would like to see a clarification on what is intended by phrase "shall make available" that is included in measures for each standard and whom an entity is supposed to make documents available to. The change from a three year retention for documents to a non-specific period will provide additional burden to the compliance process, since the region will have an arbitrary time length assigned per specific incident.
Individual
Jianmei Chai
Consumers Energy Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southern California Edison Company
Rebecca Furman
Law Department
Yes

	No
	R1.3 - Add language to indicate whether Senior Manager may or may not delegate annual review and approval of the policy. R3.2 - SCE believes that the removal of “acceptance of risk” limits SCE’s ability to analyze risk and determine a proper response. For example, SCE could determine that the residual risk posed by the state of maturity of a technology used to address CIP requirements is both low risk and low probability. Removing the acceptance of risk language would require SCE to continue to allocate time and resources to address the residual risk rather than deeming it acceptable within the CIP Standards. SCE recommends adding language to indicate that where unavoidable residual risk remains after remediation, it must be documented and authorized by the Senior Manager or delegate.
	Yes
	Yes
	Request clarification on the difference between "process" and "procedure."
	No
	For R1.8 Annual review and approval - we interpret it as the Senior Manager or delegate reviews and approves the physical security plan annually. For consistency with R2, suggest re-wording R3 to: "Protection of Electronic Access Control Systems - Cyber Assets that authorize and/or log access to the Electronic Security Perimeter (s) shall reside within an identified Physical Security Perimeter." Delete R2.1.
	No
	The change from 90 days to 30 days is difficult to achieve. SCE suggests 60 days to provide ample time for internal due diligence.
	Yes
	Yes
	No
	Wording is ambiguous. SCE suggests "six (6) months from date of approval."
	Yes
	Yes
	Yes
	Yes
	SCE hereby submits these additional general comments and questions(not related to or in response to Question 13): 1. What is the approval process for Violation Severity Levels? Will they be part of the standards? Will they be circulated for comment as part of the approval process? 2. In the Data Retention section of each Standard, a retention period is not specified for audit records. What is the retention period?
	Group
	Tampa Electric Company
	T.J. Szelistowski
	Tampa Electric Company
	Yes
	No
	Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in

	non-compliance."
	No
	Requirement R3 The proposed changes would result in the language: "....A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency."(removing within 30 days of being granted access). This would leave the standard open to the interpretation that as long as an assessment is no older than 7 years old, then this risk assessment is “prior” to the personnel begin granted access. Tampa Electric is unsure if this is the intention of the language change. If this is not the intenct, then the wording should be clarified. Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
	No
	In R1.5, the change from “and” to “and/or” could bring unintended devices into scope of this standard. The change should be clarified to say “access control of and/or monitoring access to of the Electronic Security Perimeter(s).” Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
	No
	Requirement 1.3: Remove “processes” from the wording to be consistent with the other changes in CIP006 Requirement 1 and eliminate the redundancy of having “processes” and “procedures” in same statement. Processes are included in the procedures. Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
	No
	Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
	No
	Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
	No
	Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
	Yes
	Yes
	Yes

Yes
Yes
Group
Electric Market Policy
Jalal Babik
Dominion Resources Inc
Yes
1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Propose that section 4.2 for each standard (CIP-002-2 through CIP-009-2) be updated to state that law enforcement agencies and emergency services in the performance of their duties are exempt from the standards.
Yes
1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Suggest R3.1 read thirty calendar days.
Yes
1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2)Suggest rewording Requirement R2.1 as follows: :This program will ensure that all personnel requiring access to Critical Cyber Assets, …" for clarity.
Yes
NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Yes
1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Requirement R1.4, it is not clear what is intended by the phrase "response to loss." . 3) Requirement R1.4 should reference R4 rather than R3. 4) Suggest standardizing the language used in R4, R5 and R6. (R4 refers to security personnel; R5, second bullet, to authorized personnel; R6, third bullet, to security or other authorized personnel.)
Yes
NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Yes
NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Yes
NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Yes
NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Yes
1) "Responsible Entity" is not defined in the implementation plan. 2) On page 1 under Implementation Schedule, Item #3 should read: "A new or existing "Cyber" Asset becomes …" 3) On page 2, the first sentence should reference "other" Cyber Assets rather than "non-critical" Cyber Assets to be consistent with the red-line change to CIP-007-2 Purpose. 4) On page 4, bullet "b" permeter needs to be capatalized.
Yes
On page 6, Table 2 Milestone Categories should indicate "months."
Yes
Yes

Individual
Randy Schimka
San Diego Gas and Electric Co.
Yes
Yes
No
To help clarify training requirements for different users and access levels, SDG&E would like to see language added to CIP-004-1 R2.2 stating that training should be appropriate to user duties, functions, experience, and access level. Information concerning vulnerabilities should be revealed on a need to know basis and not universally.
Yes
No
SDG&E has the following comment to make about CIP-006-2 R2.1: This requirements states that cyber assets that authorize and/or log access to PSPs must be "protected from unauthorized physical access." In addition, R2.2 states that these cyber assets must be afforded the protective measures specified in, among others, CIP-006-2 R4, which addresses physical access control. Including both of these statements seems redundant. We recommend removing R2.1 and appending the text of R2.2 to R2 (thus allowing the deletion of R2.2)
Yes
Yes
Yes
Yes
Yes
Yes
No
For clarity, SDG&E prefers the stand-alone Implementation Plan documents as presented rather than integrating the information for newly identified CCAs and newly registered entities into the existing CIP standards. This will help eliminate confusion and keep the existing Standard requirements and new CCAs/Registered Entity information separate.
No
While the Standards Drafting Team has done a great job overall incorporating many of the issues raised in FERC Order 706 FERC, there appears to be two issues identified by FERC in Order 706 that have not been addressed by the Standards re-write team in these first revisions. FERC Order 706 directed in Paragraph 88 that features such as enhanced conditions on technical feasibility exceptions and oversight of critical asset determinations for CIP-002 are too important to the protection of the Bulk-Power System to wait until the 2009-2010 time period for the process to start. But no substantial modifications for CIP-002 in these areas are included from the SDT. In addition, FERC Order 706, in Paragraph 90, also directed the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule. This doesn't appear to have been completed by the SDT as a first priority.
Individual

Alice Druffel
Xcel Energy
Yes
No
It appears as though R3.2 could be interpreted to require compensating measures, once the phrase "or a statement accepting risk" is eliminated. We would like clarification if this was the intent.
Yes
Yes
No
Xcel Energy feels strongly that 30 days is too short of a time frame to get drawings updated, Sr. Management approval,.etc. every time there is a change to the plan. We feel that 60 calendar days is more attainable industry-wide.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Kathleen Goodman
ISO New England Inc
No
We recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. Rational: 1 - The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. 2 - Allows for, "The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall …" 3 - In this Standard and throughout several other CIP Standards, "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate and cannot be applied.
No
1 - In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundent and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice. 2 - We recommend moving CIP-003 R2 into the CIP-002 Standard. Therefore the change to APPLICABILITY 4.2.3 would not be necessary. 3 - We take acceptiopn to the inclusion of the words "single" and "authrority." These inclusions present a specific example where the CIP Standards are too prescriptive in that they seek to

	regulate company's internal management, as opposed to regulating performance. This modification is inappropriate and potentially outside NERC's legislative mandate. The drafting team must explain what it intends by adding the word "authority" to the word "responsibility." Second, if "authority" is given a meaning of having the power to ensure that capital resources are expended to achieve the objectives laid out in the Standard, we have questions about how NERC can propose regulating how companies manage their budgets. Some companies budgets must be approved by their Boards, and some companies' budgets must be approved by FERC. 4 - We suport the change to R2.1 5 - We request clarification of CIP-003 R2.3. Would very short term delegations (less than 30 days) for vacation and out-of-office travel need same level of recording and Senior Manager approval. 6 - In this Standard and throughout several other CIP Standards, the lead focus statement in the Measures is re-stated redundently throughout each of the bulleted Measure statements. Please clean-up such text.
	No
	1 - In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundent and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice.
	No
	1 - "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. 2 - R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.
	No
	1 - We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2 - We request a correction to R1.4 which references R3. We believe this is now R4. 3 - Regarding R1.6, we are concerned with the new word "continuous." it is subjective and will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4 - We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"
	No
	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
	No
	1 - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop. and maintain a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident, when such an incident occurs." 2 - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within within thirty calendar days of completion of the Entity's Change Process" 3 - The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4 - Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
	No
	1 - We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed." to "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of completion of the Entity's change process." 2 - "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate.
	No
	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While

	Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009
	No
	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entites. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some references Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of:"to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
	No
	1 - We recommend that Table 2 clarifies the units as months, per page 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
	Yes
	Yes
	1 - We agree with the removal of "reasonable business judgment" and "acceptance of risk." 2 - GENERAL COMMENT: As a general matter, NERC needs to explain how it plans on enforcing these standards. This is critical, because NERC is not defining what cyber-security practices are, in fact, acceptable. Therefore, if a company establishes a "high bar for its internal programs (e.g., training employees), and does not meet its own business practices, it can be fined by NERC. By contrast (and depending on how the standards are enforced) companies that set "low bars" for its internal programs will escape penalty. NERC could inadvertently, through its compliance and enforcement policy, incent companies to establish "lowest common denominator" practices.
	Individual
	Jason Shaver
	American Transmission Company
	Yes
	Yes
	Yes
	Yes
	Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
James W. Sample
TVA
No
There are three areas we feel need clairification: 1) Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements; 2) delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard; and 3) an appoint of a senior manager is a part of CIP-003 and for Responsible Entities without Critical Assets only CIP-002 is applicable. We propose the following: 1) R4 be revised to: Annual Approval — The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) 2) Move the senior manager appointment from CIP-003 R2 to CIP-002. 3) Incorpoarte, by reference to CIP-003, for a senior manager appointment into CIP-002.
Yes
Yes
Yes
No
We agree with all except, CIP-006 R1.6. CIP-006 R1.6 requires a "continuous" escort. We agree that performing escort duties in a manner that ensures visitors actions are supervised and malicious attempts are prevented is critical. However, being able to provide auditable proof of "continuous" escorting creates a condition that is impossible to meet. We propose the following: R1.6: Policy and procedures describing roles, responsibilities, and corrective action in regard to escorting personnel not authorized for unescorted access within the Physical Security Perimeter. We would also recommend that Responsible Entitie obtain a signature for record from individuals performing escort duties demonstrating that they acknoweledge and accept their role and responsbilities and understand what corrective actions will be taken for any breach in procedure.
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
PPL Corporation
Annette M. Bannon
PPL Supply
Yes
Yes
Yes
Yes
No
Recommend a correction to R1.4 which references R3. We believe this is now R4.
Yes
We fully support the revisions in section B, Requirements.
No
The sentence added to the end of R1.6 would be more appropriate in a FAQ, guideline, or interpretation rather than in the standard itself.
Yes
Yes
Yes
PPL agrees with different categories of newly identified Critical Cyber Assets and the different implementation schedule for these classes of categories.
No
PPL has concerns with the existing implementation schedule. Table 2 identifies some standard requirements as existing for Category 2 milestones. Having an Information Protection program does not mean that all information associated with a newly identified Critical Cyber Asset is immediately protected. For example, if an RE identifies an asset as critical with critical cyber assets, not all drawings and documentation will exist immediately marked as such.

Even existing programs need to be applied to newly identified assets requiring an implementation schedule. The second concern is dependent on the outcome of the FERC Order for Clarification of CIP standards applicability to nuclear generating facilities. If the FERC Order results in nuclear facilities being included in the CIP applicability, this implementation plan should be noted to not include nuclear facilities affected by the pending FERC Order. The FERC Clarification Order needs to address the schedule for including nuclear facilities in the CIP applicability.
Yes
Yes
Group
MRO NERC Standards Review Subcommittee
Michael Brytowski
MRO
No
The MRO NSRS believes that R4 is prescriptive in nature. The requirement tells how to accomplish, not what to accomplish.
No
The MRO NSRS believes the R2 should be moved to CIP-002. This would package all of the requirements in one standard the apply to every entitiy. The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
Yes
No
On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4. The MRO NSRS proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.
No
The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4. The MRO NSRS proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party. The MRO NSRS agrees with the remaining changes in CIP-006-2.
No
The MRO NSRS do not agree with the change within the Purpose section of the standard to change the term “non-critical” to “other.” The term "other" is too vague. The MRO NSRS proposes the following language: Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets

	used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
	No
	The MRO NSRS questions the change in timing requirements for R1.4 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan not being updated within 90 days.
	No
	The MRO NSRS questions the change in timing requirements for R3 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan(s) not being updated within 90 days.
	Yes
	Yes
	Yes
	Yes
	No
	The new effective date goes above the requirements listed in order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
	Individual
	Greg Rowland
	Duke Energy
	Yes
	No
	We believe that R3.2 should be revised to require an analysis of risk, in order to provide understanding of what the compensating measures are achieving. Suggested language is as follows: "Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary, any compensating measures, and analysis of residual risk."
	Yes
	Yes
	No
	The language introduced in R2 and R3 has created an inconsistency with the use of the phrases "authorize and/or log access" and " access control and/or monitoring". This creates confusion and opportunity for differing interpretations of the requirements.
	Yes
	Regarding R2.3, R3.2 and R4.1, we understand that the Responsible Entity's action to document compensating measures is sufficient to achieve compliance with the requirements, and that the Responsible Entity does not need to also invoke the "Technical Feasibility" exception. Technical Feasibility is only applicable when the Responsible Entity cannot comply with a requirement. We also recommend that the Responsible Entity be required to perform an analysis of the residual risk after all compensating measures are applied. Add the words "and analysis of residual risk" to the end of R2.3, R3.2 and R4.1
	Yes
	Yes

Yes
Yes
Yes
Yes
Yes
Individual
Tony Kroskey
Brazos Electric Power Cooperative, Inc.
No
Suggest that the first sentence of R4 be re-written as follows: R4 The Responsible Entity shall assign a single senior manager with overall responsibility and authority for approving annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets.
No
Under the Applicability section it makes no sense for a Responsible Entity to have to comply with CIP003 R2 when there are no CCAs. This should be deleted.
Yes
Yes
No
In R1.3, replace "the perimeter(s)" with "the Physical Security Perimeter(s)". In R8.3, need to clarify what "outage records" are. In M2, replace "shall make available documentation that" with "shall make available documentation showing how" In M3, replace "shall make available documentation that" with "shall make available documentation showing how".
No
In R5.1.1, replace "user accounts" with "user access privalges". In R6.4, replace "all logs" with "all logs of system events related to cyber security". In M2, replace "available documentation" with "available documentation of all ports and services".
No
In R1.3, replace "Process for reporting" with "Process for communicating reportable". In R1.4, replace "of any changes" with "of any procedural changes". In M2, replace "all documentation" with "all relevant documentation related to Cyber Security Incidents".
No
In R3, replace "being completed" with "being effective".
Yes
Yes
Group

	Pepco Holdings, Inc - Affiliates
	Richard Kafka
	Pepco Holdings, Inc.
	No
	We appreciate and support the CSO706 SDT efforts. We agree and support the following proposed changes in CIP-002-2 through CIP-009-2: 1. Nomenclature and clarification changes (e.g. changing RRO to Regional Entity, version references) 2. Clearly state that requirements not only need a program but need to be implemented (e.g. electronic access controls, awareness program, Security Patch Management program) 3. Removed the term “reasonable business judgment” 4. Where applicable, removed the phrase “acceptance of risk” 5. Added annual review and approval of risk-based assessment methodology 6. Background checks and training would be required prior to allowing unescorted physical access or cyber access to critical cyber assets (i.e. eliminates 90 days or 30 days after the fact but allows for emergencies) 7. Added protection of physical access control systems However we have the following questions about changes in CIP-002-2. (These questions also apply to CIP-003-2 through CIP-009-2 but will not be repeated below.): 1. The proposed change for D. Compliance, Section 1.1 appears to add a new term, "Compliance Enforcement Authority", (which we do not believe is in the Glossary of Terms or in any other standards as of 12/1/08). Does the CSO706 SDT plan to define this new term? If yes, how will it be different from the term "Compliance Monitor" (defined in the Glossary of Terms)? 2. In D. Compliance, Section 1.1.2 The proposed change is to replace NERC with ERO. We believe that this should be left as NERC as we do not believe ERO appears in the Glossary of Terms or in any other standards. If ERO remains, does ERO need to be added to the applicability list in A. Introduction, Section 4.1 and the Glossary of Terms?
	Yes
	We support the proposed modifications including the removal of business phone and business address from B. Requirements, R2.1. Similary, should the business phone requirement be removed from B. Requirements, R5.1.1? Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-003-2, D. Compliance, Section 1.5 say "None"?
	Yes
	We agree with the proposed modifications especially with the phrase "except in specified circumstances such as an emergency". Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-004-2, D. Compliance, Section 1.5 say "None"?
	Yes
	No
	It may not be possible to communicate updates of recovery plans to all personnel responsible for activating or implementing the plan within 30 days (e.g. family leave). Suggest adding exceptions.
	Yes
	Please consider adding in parenthesis "approximately 270 days" after "the third calendar quarter" for clarification. "The first day of the third calendar quarter (approximately 270 days) after applicable approvals..."
	Yes
	We specifically appreciate and support the CSO706 SDT efforts in closing the current gap in the CIP standards for compliance of newly identified Critical Cyber Assets by creating three categories with a related implementation schedule.
	Yes
	In response to the CSO706 SDT question, we agree that the implementation plan for newly identified Critical Cyber Assets should be incorporated into the cyber security standard and belive that it should be included as part of CIP-002-1).
	No
	1. We understand that the SDT is proposing that Technical Feasibility Exceptions (TFE) Process (i.e. exception approval process) be modeled after the existing Self-Report and

	Mitigation Plan processes in the Compliance Monitoring and Enforcement Program (CMEP) which would require TFE review by the Regional Entity and NERC to assess the impact to the BES and then approve or not approve the exception. We also understand that as part of the NERC TFE approval process a mitigation plan would need to be submitted to the Regional Entity/NERC and completed for compliance. We understand that the Standards Drafting Team (SDT) is proposing that the TFE process be done through the NERC Rules of Procedure update process rather than through the standards process. 1. Is it the intent of the SDT is to keep the TFE process outside of the compliance process (i.e. TFE requirement as part of the NERC Rules of Procedures)? 2. The existing Self-Report and Mitigation Plan process is for self-reporting and remedying a potential non-compliance. Is the intent of modeling the existing Self-Report and Mitigation Plan for the TFE process because the SDT considers Technical Feasibility Exceptions as non-complicance to the CIP standards? It was our understanding that TFEs are not a compliance issue. The existing FAQs state: Technical feasibility refers only to engineering possibility and is expected to be a “can/cannot” determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by the Responsible Entity. The Responsible Entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf 3. We believe that the TFE process needs to be included in the standards as well (e.g. CIP-003-2 R3). If the TFE is not coupled to the Standards (e.g. requirement to submit to RE and NERC for approval) we have concerns that there may be unintended gaps or conflicts. 1. For example what happens if a Registered Entity in following CIP-003-2 R3 (Exceptions) has a technical exception approved by the Sr. Manager but by a de-coupled TFE process NERC does not approve the exception? The Registered Entity is in compliance with the Standard but not with the TFE approval process. Would failure of a TFE procedure be considered non-compliance and therefore subject to fines? 2. Another example of a potential gap or conflict is there could be conflicting effective dates of the standards and the TFE process (i.e. the requirement to submit to NERC for approval) if these are not linked together. 3. Timing of the approvals by NERC could also create a gap or conflict. 4. We encourage the SDT drafting team to consider including the requirement of RE/NERC review in the standards. The detailed process and procedures could be separate. 5. Finally we believe that the SDT needs to identify how the RE and/or NERC will perform the assessment of a TFE request on the impact to the BES (e.g. engineering judgement, load flow studies, stability studies,...) and identify the parameters that would be considered an approved exception versus an unapproved exception. 2. We understand and agree that NERC has the right to review TFE information and evidence of compliance but providing this information/data offsite may be considered a violation to the CIP requirement(s) and at the very least is a potential risk because if this information is compromised could show vulnerabilities to Critical Cyber Assets at a given Registered Entity. The confidentiality and security of the data/information needs to be considered. Potential options could include: 1. NERC could review information over a secure communication channel without NERC keeping the sensitive information

Consideration of Comments on 1st Draft of CIP-002-2 through CIP-009-2 — Project 2008-06 — Cyber Security Order 706

The Cyber Security Standards Drafting Team for the revisions to the standards resulting from FERC Order 706 and Order 706A thanks all commenters who submitted comments on the first draft of the following CIP standards:

CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards were posted for a 45-day public comment period from November 21, 2008 through January 5, 2009. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 52 sets of comments, including comments from more than 100 different people from over 55 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

The extensive scope of Project 2008-06 Cyber Security Order 706 has led the Cyber Security Standards Drafting Team to develop a multiphase strategy to revise the CIP Standards (CIP-002 through CIP-009) and the Implementation Plan.

Phase 1 of the project includes the necessary modifications to the CIP Standards (CIP-002-1 through CIP-009-1) and the Implementation Plan to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards, are also addressed in Phase 1. The more contentious issues will be addressed by the SDT in subsequent phase(s) of Project 2008-06 Cyber Security Order 706.

Based on the recent stakeholder comments, the Cyber Security Standards Drafting Team made the following modifications to the CIP Standards (CIP-002 through CIP-009) and Implementation Plan:

- Revised the Access Control requirement (R5.1.1) in Standard CIP-003-2 to delete the inclusion of business phone information as part of the identification of the designated personnel who are responsible for authorizing logical or physical access to protected information.

- Revised the Awareness requirement (R1) in Standard CIP-004-2 to clarify that the Responsible Entity shall establish, document, implement, and maintain, a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

- Revised the Training requirement (R2) in Standard CIP-004-2 to clarify that the Responsible Entity shall establish, document, implement, and maintain, an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

- Revised the Personnel Risk Assessment requirement (R3) in Standard CIP-004-2 to clarify that the Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

- Revised the Electronic Access Controls requirement (R2.3) in Standard CIP-005-2 to clarify that the Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

- Revised the Measures (M1 through M5) included in Section C of Standard CIP-005-2 to clarify that the documentation to be made available by the Responsible Entity as a measure of compliance to the standard does not need to be dated.

- Revised the Physical Security Plan requirement (R1) in Standard CIP-006-2 to clarify that the Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s).

- Revised the Purpose statement included in Standard CIP-007-2 to clarify that Responsible Entities will define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

- Revised Measure M1 of Standard CIP-008-2 to clarify that the Cyber Security Incident response plan to be made available by the Responsibility Entity is not required to be dated.

- Revised the Measures (M1 through M5) included in Section C of Standard CIP-009-2 to clarify that the recovery plan(s) and related documentation to be made available by the Responsible Entity as a measure of compliance to the standard do not need to be dated.

- Revised the Implementation Plan for the CIP-002-2 through CIP-009-2 cyber security standards to clarify the formula to determine the “effective date” of the standards for each stakeholder and to provide an example of the calculation.

- The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was updated to identify the schedule for becoming compliant with the requirements of the Cyber Security Standards (CIP-003-2 through CIP-009-2) and their successor standards, once an Entity’s applicable ’Compliant‘ milestone date listed in the existing Implementation Plan has passed.

In this report, the comments have been sorted so it is easier to see where there is industry consensus on the questions posed and where possible issues remain to be resolved through future phases and subsequent releases of the standards.

The latest status and information related to Project 2008-06 Cyber Security FERC Order 706 can be found on the NERC Website at the following URL address:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Individual	Kent Kujala	Detroit Edison Company			✓		✓					
2.	Individual	Paul Golden	PacifiCorp	✓		✓		✓					
3.	Group	Doug Hohlbaugh	FirstEnergy Corp	✓		✓	✓	✓	✓				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	1, 3, 4, 5, 6
2.	Terry Malone	FE	RFC	1, 3, 4, 5, 6
3.	Karen Yoder	FE	RFC	1, 3, 4, 5, 6
4.	Dave Folk	FE	RFC	1, 3, 4, 5, 6
5.	Henry Stevens	FE	RFC	1, 3, 4, 5, 6

4.	Individual	Ray Andrews	MidAmerican Energy Company	✓		✓		✓					
5.	Group	Guy Zito	Northeast Power Coordinating Council										✓

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Edward Dahill	National Grid	NPCC	3
2.	Gerald Mannarino	NYPA	NPCC	5
3.	Frederick White	Northeast Utilities	NPCC	1
4.	Michael Garton	Dominion Resources Services, Inc.	NPCC	5
5.	Kathleen Goodman	ISO - New England	NPCC	2
6.	Michael Gildea	Constellation Energy	NPCC	6
7.	Donald Nelson	Massachusetts Dept. of Public Utilities	NPCC	9
8.	Roger Champagne	Hydro-Quebec TransEnergie	NPCC	1
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1
10.	Brian Hogue	NPCC	NPCC	10
11.	Gerry Dunbar	NPCC	NPCC	10
12.	Lee Pedowicz	NPCC	NPCC	10
13.	Brian Evans-Mongeon	Utility Services	NPCC	6

6.	Individual	Linda Perez	WECC Reliability Coordination										✓
7.	Group	Marc M. Butts	Southern Company	✓		✓		✓	✓				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rodney O'Bryant	Southern Company Services	SERC	1
2.	Larry Spoonemore	Southern Company Services	SERC	5
3.	Jim Busbin	Southern Company Services	SERC	1
4.	Bonnie Parker	Southern Company Services	SERC	5
5.	Boyd Nation	Southern Company Services	SERC	1
6.	Wes Stewart	Southern Company Services	SERC	1
7.	Bob Canada	Southern Company Services	SERC	1
8.	Wade Mundy	Southern Company Services	SERC	1
9.	John Greaves	Georgia Power Company	SERC	1, 3
10.	Jay Cribb	Southern Company Services	SERC	1
11.	Chris Wilson	Southern Company Services	SERC	1

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	12. Terry Coggins — Southern Company Services — SERC — 1 13. Russ Ward — Southern Company Services — SERC — 1 14. Steve Bennett — Georgia Power Company — SERC — 1, 3 15. Larry Smith — Alabama Power Company — SERC — 1, 3											
8.	Individual	Rick Terrill	Luminant Power					✓						
9.	Group	Matthew E. Luallen	Encari								✓			
	Additional Member / **Additional Organization** / **Region** / **Segment Selection** 1. Steve Hamburg — Encari — NA - Not Applicable — 8 2. Mark Simon — Encari — NA - Not Applicable — 8 3. Lenny Mansell — Encari — NA - Not Applicable — 8 4. Peter Brown — Encari — NA - Not Applicable — 8											
10.	Individual	Mark Phillips	TransAlta Centralia Generation, LLC					✓						
11.	Group	Denise Koehn	Bonneville Power Administration	✓		✓		✓	✓					
	Additional Member / **Additional Organization** / **Region** / **Segment Selection** 1. Curt Wilkins — Transmission System Operations — WECC — 1 2. Bradley Folden — Transmission Technical Training — WECC — 1 3. Kelly Hazelton — Transmission Control Cntr HW Design & Maint — WECC — 1											
12.	Individual	John Lim	Consolidated Edison Company of New York, Inc.	✓		✓		✓	✓					
13.	Individual	Rebecca Furman	Southern California Edison Company	✓		✓		✓	✓					
14.	Individual	T.J. Szelistowski	Tampa Electric Company	✓		✓		✓						
15.	Group	Jalal Babik	Electric Market Policy	✓		✓		✓	✓					

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Louis Slade	Electric Market Policy	RFC	6
2.	Mike Garton	Electric Market Policy	NPCC	5
3.	Mark Engels	IT Risk Management	SERC	
4.	Ruth Blevins	IT Risk Management	SERC	
5.	Dennis Sollars	IT Risk Management	SERC	
6.	John Albert	Security Compliance	SERC	

16.	Group	Annette M. Bannon	PPL Corporation	✓				✓	✓				

Please complete the following information.

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Heimbach	PPL EnergyPlus	MRO	6
2.			NPCC	6
3.			RFC	6
4.			SERC	6
5.			SPP	6
6.	Jim Batug	PPL Generation	NPCC	5
7.			RFC	5
8.			WECC	5
9.	Barry Skoras	PPL Electric Utilities	RFC	1

17.	Group	Michael Brytowski	MRO NERC Standards Review Subcommittee										✓

	Additional Member	Additional Organization	Region	Segment Selection
1.	Neal Balu	WPS	MRO	3, 4, 5, 6
2.	Terry Bilke	MISO	MRO	2
3.	Carol Gerou	MP	MRO	1, 3, 5, 6
4.	Jim Haigh	WAPA	MRO	1, 6
5.	Charles Lawrence	ATC	MRO	1
6.	Ken Goldsmith	ALTW	MRO	4

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	7. Terry Harbour	MEC	MRO	1, 3, 5, 6										
	8. Pam Sordet	XCEL	MRO	1, 3, 5, 6										
	9. Dave Rudolph	BEPC	MRO	1, 3, 5, 6										
	10. Eric Ruskamp	LES	MRO	1, 3, 5, 6										
	11. Joseph Knight	GRE	MRO	1, 3, 5, 6										
	12. Larry Brusseau	MRO	MRO	10										
	13. Scott Nickels	RPU	MRO	3, 4, 5, 6										
18.	Group	Richard Kafka	Pepco Holdings, Inc - Affiliates		✓		✓		✓	✓				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
	1. Mark Godfrey	Pepco Holdings, Inc.	RFC	1										
19.	Individual	Michael Puscas	United Illuminating Company		✓		✓							
20.	Individual	Steven Dougherty	Deloitte& Touché, LLP											
21.	Individual	Chris Scanlon	Exelon		✓		✓		✓	✓				
22.	Individual	Mark Ringhausen	Old Dominion Electric Cooperative					✓						
23.	Individual	Alan Gale	City of Tallahassee (TAL)		✓		✓		✓					
24.	Individual	Brian Martin	BC Transmission Corporation		✓	✓								
25.	Individual	Joe Weiss	Applied Control Solutions, LLC											
26.	Individual	Martin Bauer	US Bureau of Reclamation		✓				✓					
27.	Individual	Edward Bedder	Orange and Rockland Utilities Inc.		✓									
28.	Individual	Martin Narendorf	CenterPoint Energy		✓									
29.	Individual	Kris Manchur	Manitoba Hydro		✓	✓		✓	✓					

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
30.	Individual	Anita Lee	Alberta Electric System Operator		✓								
31.	Individual	Greg Mason	Dynegy					✓					
32.	Individual	Tim Conway	Northern Indiana Public Service Company	✓		✓		✓					
33.	Individual	Robert Huffman	CoreTrace								✓		
34.	Individual	Darryl Curtis / Greg Ward	Oncor Electric Delivery LLC	✓									
35.	Individual	Bob Thomas	Illinois Municipal Electric Agency				✓						
36.	Individual	Cathie Mellerup	Ontario Power Generation					✓					
37.	Individual	Jim Sorrels	American Electric Power	✓		✓		✓	✓				
38.	Individual	Dan Rochester	Ontario IESO		✓								
39.	Individual	Kirit Shah	Ameren	✓		✓		✓	✓				
40.	Individual	Jianmei Chai	Consumers Energy Company			✓	✓	✓					
41.	Individual	Alice Druffel	Xcel Energy	✓		✓		✓	✓				
42.	Individual	Kathleen Goodman	ISO New England Inc		✓								
43.	Individual	Jason Shaver	American Transmission Company	✓									
44.	Individual	James W. Sample	TVA	✓		✓		✓	✓				
45.	Individual	Greg Rowland	Duke Energy	✓		✓		✓	✓				
46.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	✓									

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
47.	Group	Ed Goff	Progress Energy	✓		✓		✓	✓				
48.	Group	Ben Li	Standards Review Committee of ISO/RTO Council										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Patrick Brown	PJM	NPCC	2
2.	Jim Castle	NYISO	NPCC	2
3.	Matt Goldberg	ISONE	NPCC	2
4.	Lourdes Estrada-Salinero	CAISO	WECC	2
5.	Anita Lee	AESO	WECC	2
6.	Steve Myers	ERCOT	ERCOT	2
7.	Bill Phillips	MISO	RFC	2
8.	Charles Yeung	SPP	SPP	2

49.	Individual	Aldo Nevarez	KEMA										
50.	Individual	Dave DeGroot	Austin Energy	✓				✓					
51.	Individual	Glen Hattrup	Kansas City Power & Light	✓		✓		✓					
52.	Individual	Randy Schimka	San Diego Gas and Electric Co.	✓		✓	✓	✓					

1. The CSO706 SDT added management approval of the risk-based assessment methodology (per FERC Order 706, paragraph 236) to **CIP-002-1 Requirement R4**. Do you agree with the proposed modification? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

While about half of the stakeholders provided commented feedback to the CIP-002 Requirements, the overwhelming issue that was raised concerned a better organization of the CIP-002 and CIP-003 Requirements. The commenters suggested a reorganization such that all of the Requirements that all Entities must complete be collected in one standard (CIP-002).

Many comments referred to the definition of the Senior Manager, his/her role, and his/her responsibilities. These were clarified by the SDT in its responses.

Other significant comments addressed the designation of the "enforcement authority" role to the appropriate Responsible Entities, removal of "dated" from the measurements, the required management approval of the risk-based assessment methodology that is utilized, and the removal of "reasonable business judgement" from the standards. The SDT clarified the designation of the enforcement authority role in its responses, and agreed to remove "dated" from the measures defined in the standards.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards

The SDT made the following modification to the standard, based on stakeholder comments:

M2, M3, and M4: The word "dated" was removed from the Measures included in Section C.

Organization	Yes or No	Question 1 Comment
Standards Review Committee of ISO/RTO Council	No	(1) Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements. Further, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 be revised to: "Annual Approval — The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)" If appointing a senior mangager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4

Organization	Yes or No	Question 1 Comment
		should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. (2) In this Standard and throughout several other CIP Standards, "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate and cannot be applied.
Response: (1) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. (2) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
TVA	No	There are three areas we feel need clarification: 1. Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements; 2. Delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard; and 3. An appointment of a senior manager is a part of CIP-003 and for Responsible Entities without Critical Assets only CIP-002 is applicable. We propose the following: i) R4 be revised to: Annual Approval - The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. ii) The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) iii) Move the senior manager appointment from CIP-003 R2 to CIP-002. Incorporate, by reference to

Organization	Yes or No	Question 1 Comment
		CIP-003, for a senior manager appointment into CIP-002.
Response: i). The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. (Reference FERC Order 706 Paragraph 381) ii). The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity. (reference FERC Order 706, Paragraph 381) iii). As stated in CIP-003-2, all Responsible Entities regardless of a null Critical Cyber Asset list are required to perform CIP003-2 R2.		
Brazos Electric Power Cooperative, Inc.	No	Suggest that the first sentence of R4 be re-written as follows: R4 The Responsible Entity shall assign a single senior manager with overall responsibility and authority for approving annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets.
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Ontario IESO	No	Standards should hold a functional entity(ies) responsible for meeting the requirements, not a person or a position. Furthermore, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 be revised to: "Annual Approval? The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) "If appointing a senior manager is required to ensure standards are complied with and implemented, we

Organization	Yes or No	Question 1 Comment
		recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. The senior manager is held responsible to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation needs to be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS believes that R4 is prescriptive in nature. The requirement tells how to accomplish, not what to accomplish.
Response: The SDT respectfully disagrees with the comment. CIP-002-2 R4 is a requirement for governance over the critical cyber asset identification standard. The SDT's intent was to define annual approval by the senior manager.		
US Bureau of Reclamation	No	The modification of the standard to require that a specific individual approve the risk-assessment methodology appears to be overstepping the bounds of the authority of the regulatory agencies as it pertains to improved reliability. It is difficult to imagine or prove that having one individual within an agency approve a methodology (as opposed to making the entity responsible for having and using a methodology) improves system reliability. Such a requirement is also not consistent with most of the other BES reliability standards. For consistency, the standard should refer to "Responsible Entity" rather than specific individuals within the organization. That determination is the sole discretion of the Responsible Entity and was not required by FERC. FERC required, in paragraph 236, that "internal, management, approval of the riskbased assessment" is required. FERC further clarified: "A responsible entity, however, remains responsible to identify the critical assets on its system". To that end the standard should require that the 'Responsible Entity" ensure that management has approved the risk based assessment. The "Responsible Entity" is then responsible to demonstrate that the requirement has been met and who approved it.

Organization	Yes or No	Question 1 Comment
Response: The intent of the standard is not to define an entity's organizational structure. The intent is to ensure that the appropriate governance structure is taken into consideration and that, as directed by FERC, there exists a single individual with overarching authority.		
Alberta Electric System Operator	No	The functional entity (e.g. the Balancing Authority, etc) should be designated as the responsible entity for this requirement, not an individual. This would be consistent with other ERO standards. Also, R1 implies that the purpose of this standard is not only to identify the "Critical Cyber Assets" but also the "Critical Assets" (which must be done before you can identify the Critical Cyber Assets), and hence we suggest that either the identification of "critical Assets" be specified in its own and separate standard or the Title and Purpose of CIP-002 be clarified to state that there are 2 purposes to this standard. We suggest that R1 should be re-written to improve clarity. R1, as currently written, contains not only a single requirement, but has at least two and possibly three or more requirements embedded in it. The accountabilities for these different requirements could be different within an organization, so assigning those to one person would be inappropriate.
Response: The change made in CIP-002 includes adding the management approval of the risk-based assessment methodology per directives in FERC Order 706. Given the limited scope and timeline for Phase 1, please re-address the additional concerns during the Phase 2 comment period.		
Pepco Holdings, Inc - Affiliates	No	We appreciate and support the CSO706 SDT efforts. We agree and support the following proposed changes in CIP-002-2 through CIP-009-2: 1. Nomenclature and clarification changes (e.g. changing RRO to Regional Entity, version references) 2. Clearly state that requirements not only need a program but need to be implemented (e.g. electronic access controls, awareness program, Security Patch Management program) 3. Removed the term "reasonable business judgment" 4. Where applicable, removed the phrase "acceptance of risk" 5. Added annual review and approval of risk-based assessment methodology 6. Background checks and training would be required prior to allowing unescorted physical access or cyber access to critical cyber assets (i.e. eliminates 90 days or 30 days after the fact but allows for emergencies) 7. Added protection of physical access control systems However we have the following questions about changes in CIP-002-2. (These questions also apply to

Organization	Yes or No	Question 1 Comment
		CIP-003-2 through CIP-009-2 but will not be repeated below.): 1). The proposed change for D. Compliance, Section 1.1 appears to add a new term, "Compliance Enforcement Authority", (which we do not believe is in the Glossary of Terms or in any other standards as of 12/1/08). Does the CSO706 SDT plan to define this new term? If yes, how will it be different from the term "Compliance Monitor" (defined in the Glossary of Terms)? 2). In D. Compliance, Section 1.1.2 The proposed change is to replace NERC with ERO. We believe that this should be left as NERC as we do not believe ERO appears in the Glossary of Terms or in any other standards. If ERO remains, does ERO need to be added to the applicability list in A. Introduction, Section 4.1 and the Glossary of Terms?
Response: 1) The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures. 2) Under the ERO Rules of Procedure, the ERO can be penalized but not NERC – therefore the use of the term, "Electric Reliability Organization" or "ERO" is technically correct. As a guideline, drafting teams are asked not to add terms to the glossary unless there is a chance that the term will be misunderstood. In this case, the entities who follow these standards should know what is meant by these terms, and we don't believe the terms need to be added to the glossary.		
Southern Company	Yes	CIP-002 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-002 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-002 Section D - Compliance: 1.4.2- Should have a time limit to reduce the overall liability of confidential information.
Response: 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405). 1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C –		

Organization	Yes or No	Question 1 Comment
Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT. 1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.		
Encari	No	1. R4 should also include a direct reference to CIP-003-2 R2 to ensure that the Responsible Entities are aware are all applicable requirements. A Responsible Entity that identifies a null CA list must still perform CIP-003-1 R2. This would allow the exemption in CIP-003-2 (4.2.3) to be removed. General Comment Provided in All Submissions--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Response:

1. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.
2. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.
3. The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.

   The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.

Organization	Yes or No	Question 1 Comment
Northern Indiana Public Service Company	No	I do support the recommended change to require management approval of the risk-based assessment methodology per FERC Order 706, paragraph 236. I would like to recommend the addition of some language to CIP-002-2 Req 4. Currently the language in R4 directs the responsible entity to comply with CIP-002-2 R1-R3 and retain a record of the resulting CA and CCA asset list (even if that list is null). My concern is that if the list is null the entity may feel they have completed all necessary actions for compliance. There is however compliance actions for an entity with a null list contained within CIP-003-2. As it stands there is an oddly placed exemption in the applicability section of CIP-003 4.2.3. I would recommend the inclusion of language in CIP-002-2 Req. 4 to identify the need for compliance with CIP-003-2 R2 as well as the currently referenced CIP-002-2 R1-3; in order to contain all applicability for CIP-002-2 R4 in one location and in turn removing the exemption in CIP-003-2. As there is no other means through the use of this comment form I would also like to comment on changes made in CIP-002-2 that repeat throughout CIP-002-2 - CIP-009-2. In the purpose section of CIP-002-2, I would like to see as a component of this draft, an attempt to develop alternative language to replace reasonable business judgment as mentioned in Order 706 in paragraph 135. In the Data Retention section of CIP-002-2, I would like to request clarification on the language added to 1.4.2. As the language was there was a limit on data retention that matched the audit enforcement period of three years. The language provided currently removes this limit and extends the retention into perpetuity as well as leaving it unclear which entity is responsible for retaining the data into perpetuity.

Response:

The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

The removal of “reasonable business judgment” was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.

The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.

Organization	Yes or No	Question 1 Comment
Consolidated Edison Company of New York, Inc.	No	We agree with the proposed modification, but have suggestions which affect CIP-002 in one area of the Leadership requirement which would be more logical.CIP-002 requires the approval of the Senior Manager for many requirements, and is the standard that determines whether other CIP standards are applicable to the Entity. In order to streamline compliance filing in these cases, and also as a more logical place for the identification of a Senior Manager, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. 1 - The senior manager has not been identified in CIP-002. Many requirements make reference to the Senior Manager or delegate. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. This is the preferred option. 2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall?
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Dynegy	No	Agree with requiring management approval of the risk-based assessment methodology. Also, suggest moving CIP-003, R2 into CIP-002 so that all the Requirements that all Entities must comply with are in one Standard.
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
ISO New England Inc	No	1) - We recommend that CIP-002 be updated by: moving CIP-003 R2 into CIP-002 or CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. Rational:

Organization	Yes or No	Question 1 Comment
		2) - The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. Allows for, "The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements" shall" 3) In this Standard and throughout several other CIP Standards, "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate and cannot be applied.
Response: 1) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 2) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity. 3) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Northeast Power Coordinating Council	No	We recommend that CIP-002 be updated by moving CIP-003 R2 into CIP-002. By moving CIP-003 R2 into CIP-002 all the Requirements that all Entities must complete are in one Standard. The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into the CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone.
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Orange and Rockland Utilities Inc.	No	We recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.1 –

Organization	Yes or No	Question 1 Comment
		The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone.2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall?
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Ontario Power Generation	No	Measures M2 and M3 add a requirement by specifying the lists of Critical Assets and Critical Cyber Assets must be dated. M2 references Requirement R2 and M3 references Requirement R3. Neither R2 or R3 require a list to be dated.
Response: The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Applied Control Solutions, LLC	No	Need to include the NIST Framework in addition to senior management approval
Response: The SDT plans to consider the NIST Framework during future phases of standards review, as directed by FERC Order 706.		

Organization	Yes or No	Question 1 Comment
American Electric Power	Yes	Section R4 of the Requirements category does not clearly define what type of unit the senior manager represents. We would suggest a clarifying comment like "for each responsible entity" be added following the word "delegate(s)." This does not appear again in any of the following standards. However, throughout all of these standards, the drafting team has introduced a new term in its use of "Responsible Entity." If this term is to be used, it should probably be considered by the NERC organization with corresponding updates to lists of compliance term glossaries and/or definitions.
Response: The SDT believes that this change could be too prescriptive and limits the flexibility allowed in delegation. "Responsible Entity" is defined within the Applicability section of each CIP standard.		
City of Tallahassee (TAL)	Yes	While I agree with the R4 revision, I disagree with the removal of the "reasonable business judgement" in all the standards. While this was in response to FERC directive, it creates a one-size-fits-all approach. Every system is different, as is their Risk Assessment Procedure. This will be one of the more contentious issues. While it may be outside the perview of the SDT, the industry has not been given the information that is needed to specifically address the Auroura fiasco. All we know is someone set up a generator and "hacked" in to change the set frequency and damage ensued. We are not aware of what software was in place to protect this "asset" or what controlling software was. Can the specifics of who set up the test and the hardware/software/control systems being utilized be shared with the industry through a NERC Alert Industry Advisory? While I do not think I have my head buried in the sand about the potential for Cyber attack, I do have a problem with taking all-encompassing action with so little information on what caused the initial knee-jerk reaction. The cost of safeguarding a system against such unknown attacks, to a level that will be acceptable during an audit (a second unknown) will surely be a significant burden to many utilities. While entities have some latitude in our "methodology" in identifying Critical Assets, the fact will remain that you have to spend money on new tools and hardware to comply with the existing requirements outside of routine budget cycles at a significant impact to operations. According to the letter from Rick Sergel to the BOT of July 7, 2008 even after we spend a ton of money, we are still susceptible to attack. Without the flexibility of determining cost vs. benefit, we will overachieve the goal to "... reasonably ensure the reliability of the BPS. . ."

Organization	Yes or No	Question 1 Comment
Response: The comments concerning Aurora are outside of the aegis of the SDT. The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Propose that section 4.2 for each standard (CIP-002-2 through CIP-009-2) be updated to state that law enforcement agencies and emergency services in the performance of their duties are exempt from the standards.
Response: 1) NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws. 2) Law enforcement agencies and emergency services are not users, owners, or operators of the Bulk Power System; therefore, it is not necessary to exempt them. Their access should be included in the emergency provisions of the cyber security policy as required by the Emergency Situations Provision in CIP-003-R1.1.		
Ameren	Yes	None.
Response: Thank you for your comment.		
American Transmission Company	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Bonneville Power	Yes	

Organization	Yes or No	Question 1 Comment
Administration		
Consumers Energy Company	Yes	
CoreTrace	Yes	
Deloitte & Touche, LLP	Yes	
Detroit Edison Company	Yes	
Duke Energy	Yes	
Exelon	Yes	
FirstEnergy Corp	Yes	
Illinois Municipal Electric Agency	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
Manitoba Hydro	Yes	
MidAmerican Energy Company	Yes	
Old Dominion Electric Cooperative	Yes	
Oncor Electric Delivery	Yes	

Organization	Yes or No	Question 1 Comment
LLC		
PacifiCorp	Yes	
PPL Corporation	Yes	
Progress Energy	Yes	
San Diego Gas and Electric Co.	Yes	
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
TransAlta Centralia Generation, LLC	Yes	
United Illuminating Company	Yes	
WECC Reliability Coordination	Yes	
Xcel Energy	Yes	
CenterPoint Energy		

2. The CSO706 SDT is proposing the following modifications to **CIP-003-1**:

   - Revise Applicability 4.2.3 to specify that compliance with Requirement R2 applies to Responsible Entities that have determined they have no Critical Cyber Assets (per FERC Order 706, paragraph 376)
   - Clarify the intent of the Requirement R2 on Leadership that a senior manager be assigned with the overall responsibility and authority for cyber security matters (per FERC Order 706, paragraph 381).
   - Add Requirement R2.3 to address senior manager delegation of authority for specific actions to a named delegate.
   - Renumber the original R2.3 to R2.4.
   - Delete the phrase "or a statement accepting risk" from Requirement R3.2.(per FERC Order 706, paragraph 376)

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

In addition to the reorganization issue of CIP-002 and CIP-003, most comments received were focused on the delegation of the Senior Manager's responsibilities and authority. Several of the commenters expressed concern that requiring a single authority for approvals was being too prescriptive.

Other concerns that were raised by the commenters included removal of the "reasonable business judgment" and "acceptance of risk" language from the standards.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT made the following modification to the standard, based on stakeholder comments:

R5.1.1 Personnel shall be identified by name, title, ~~business phone,~~ and the information for which they are responsible for authorizing access.

Organization	Yes or No	Question 2 Comment
Kansas City Power & Light	No	In CIP-003 R2, internal political difficulties are created by requiring the designated senior manager to have the authority to implement the security program. Many medium to large utilities have IT departments separate from their operations or compliance departments. In order to find a manager of sufficient direct line authority, you have moved to a level within the organization where the manager will

Organization	Yes or No	Question 2 Comment
		either not have the appropriate level of knowledge to review compliance actions or will not have sufficient time to dedicate to the task. Either way, all that will occur will be a perfunctory signature on the compliance documentation which defeats multiple goals of the program. I believe most utilities will want to comply with the spirit of this provision, but the proposed phrasing will make doing so more difficult.
Response: The senior manager is held responsible to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation needs to be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity. The responsibilities of the senior manager may be delegated with the exception of approving (1) the Cyber Security Policy required by CIP-003, Requirement R1; (2) the Risk-based Assessment Methodology required by CIP-002, Requirement R1, and (3) the technical feasibility exceptions. For those instances where delegation is not permitted or not granted, the senior manager would reasonably be expected to seek the advice of technically qualified staff before giving approval.		
Alberta Electric System Operator	Yes	However, we would like to comment that the responsibility for meeting requirements in standards must lie with the functional entity, not an individual within the entity. Also, we don't believe details on how delegation is done within an entity should be included in a standard. We propose R4 be revised to: "Annual Approval". The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null).
Response: The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The intent of the SDT is to uphold the directive from Paragraph 381 of FERC Order 706 which clarifies that the senior manager is not a user, owner, or operator of the Bulk Power System who is personally subject to civil penalties pursuant to Section 215 of FPA. The SDT believes that delegation should be addressed in the CIP standards in order to ensure that the appropriate governance structure is considered by the Responsible Entity. We have received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		

Organization	Yes or No	Question 2 Comment
MRO NERC Standards Review Subcommittee	No	The MRO NSRS believes the R2 should be moved to CIP-002. This would package all of the requirements in one standard the apply to every entitiy. The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy. The SDT received a number of comments that suggested clarifications to the delegation in CIP-003-2 R2.3. The SDT discussed this specific language and did not agree that it provided clarity over the posted language in the delegation requirement.		
Southern California Edison Company	No	R1.3 - Add language to indicate whether Senior Manager may or may not delegate annual review and approval of the policy.R3.2 - SCE believes that the removal of “acceptance of risk” limits SCE’s ability to analyze risk and determine a proper response. For example, SCE could determine that the residual risk posed by the state of maturity of a technology used to address CIP requirements is both low risk and low probability. Removing the acceptance of risk language would require SCE to continue to allocate time and resources to address the residual risk rather than deeming it acceptable within the CIP Standards. SCE recommends adding language to indicate that where unavoidable residual risk remains after remediation, it must be documented and authorized by the Senior Manager or delegate.
Response: The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy. FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]		

Organization	Yes or No	Question 2 Comment
Tampa Electric Company	No	Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.		
Duke Energy	No	We believe that R3.2 should be revised to require an analysis of risk, in order to provide understanding of what the compensating measures are achieving. Suggested language is as follows: "Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary, any compensating measures, and analysis of residual risk."
Response: The SDT does not intend to prescribe an analysis of risk for all exceptions. Please re-address this issue during the Phase 2 comment period.		
Xcel Energy	No	It appears as though R3.2 could be interpreted to require compensating measures, once the phrase "or a statement accepting risk" is eliminated. We would like clarification if this was the intent.
Response: The phrase "any compensating measures" is not intended to require compensating measures. As an Entity is free to develop a Cyber Security Policy which exceeds the minimum requirements of CIP-002-2 through CIP-009-2, there exists the case where an Entity may take exception to its Cyber Security Policy, but still meet all of the CIP requirements. Consequently, the SDT concluded that it was overreaching to require compensating measures for all exceptions to the Cyber Security Policy at this time.		

Organization	Yes or No	Question 2 Comment
Consolidated Edison Company of New York, Inc.	No	1) - We recommend moving CIP-003 R2 into the CIP-002 Standard. (See comments to Question 1). 2) - We request clarification of CIP-003 R2. 3) -"the senior manager may delegate authority for specific actions to a named delegate or delegates." 4)- Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the requirements for what the delegation must contain (i.e. does it have to explicitly reference the standard and requirement?)
Response: 1)-3) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 4) The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.		
Manitoba Hydro	No	In CIP-003 R2.3 the assignment to delegate authority could be done specifically or by assignment through the entitities policies. It should not be necessary to perform specific delegation for all circumstances which necessitates additional overhead for maintaining such documentation of delegation from the senior manager. The webinar on the revisions to the CIP Standards and other recent discussions mentioned the possible creation of a new process for instances when the phrase "where technically feasible" is applied. These instances might also be exceptions to a responsible entity's cyber security policies. Any new process dealing with "where technically feasible" must be supported by additional requirements(s) in the CIP Standards. Responsible Entities should be given direction in the CIPC Standards for identifying, documenting, managing and approving internally these instances. An additional requirement based on CIP-003-1 R3 Exceptions would provide the required direction for industry. Additional requirement(s) must included prior to further industry commenting or balloting on revised CIP Standards or before any new industry process is implemented for "where technically feasible".

Organization	Yes or No	Question 2 Comment
Response: The SDT believes that the clarifications requested regarding how a delegation is performed should be determined by the entity and does not intend to prescribe a delegation process. There is no requirement to delegate. The Technical Feasibility Exception process is under development by NERC staff. Please re-address this issue during the Phase 2 comment period.		
MidAmerican Energy Company	No	Suggest an addition: The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
Response: The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy.		
Northeast Power Coordinating Council	No	1 - We recommend moving CIP-003 R2 into the CIP-002 Standard. 2 - We request clarification of CIP-003 R2. 3 "the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) and b) the delegation.
Response: 1.-2. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 3, The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.		

Organization	Yes or No	Question 2 Comment
Orange and Rockland Utilities Inc.	No	1) We recommend moving CIP-003 R2 into the CIP-002 Standard. 2) We request clarification of CIP-003 R2. 3) "the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the delegation (i.e. does it have to explicitly reference the standard and requirement?)
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.		
PacifiCorp	No	Suggested modification to R2.3"Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions assigned to the senior manager to a named delegate or delegates."
Response: The SDT received a number of comments that suggested clarifications to the delegation in CIP-003-2 R2.3. The SDT discussed this specific language and did not agree that it provided clarity over the posted language in the delegation requirement.		
Southern Company	Yes	CIP-003 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-003 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-003 Section D - Compliance: 1.4.2 - Should have a time limit to reduce the overall liability of confidential information.

Organization	Yes or No	Question 2 Comment
Response: 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405). 1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT. 1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.		
KEMA	No	Agree with all modifications, but strongly suggest rather than deleting the phrase "or a statement accepting risk" rewording it instead. Any time compensating measures are used instead of complying with established policy or standards, some residual risk is always involved, which must be acknowledged and accepted by executive management. Use wording similar to: "...any compensating measures with executive management accepting any residual security risks." This will also force individuals to develop compensating measures with adequate coverage.
Response: The SDT will consider a Risk Management Framework as defined by NIST during future phases of modifications as directed by FERC Order 706. In addition, FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]		
Encari	No	Also see comments on Question 1 pertaining to exemption 4.2.3--General Comments Provided in All Submissions--Other modifications were also made to this standard that are not included as part of the question. 1. The wording of 1.1.1 is awkward and should be modified. 2. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. 3. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Organization	Yes or No	Question 2 Comment
Response: 1. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit. 2. The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. 3. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.		
ISO New England Inc	No	1) In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundent and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice. 2) We recommend moving CIP-003 R2 into the CIP-002 Standard. Therefore the change to APPLICABILITY 4.2.3 would not be necessary. 3) We take exceptiopn to the inclusion of the words "single" and "authority." These inclusions present a specific example where the CIP Standards are too prescriptive in that they seek to regulate company's internal management, as opposed to regulating performance. This modification is inappropriate and potentially outside NERC's legislative mandate. The drafting team must explain what it intends by adding the word "authority" to the word "responsibility." Second, if "authority" is given a meaning of having the power to ensure that capital resources are expended to achieve the objectives laid out in the Standard, we have questions about how NERC can propose regulating how companies manage their budgets. Some companies budgets must be approved by their Boards, and some companies' budgets must be approved by FERC. 4) We support the change to R2.1 5) We request clarification of CIP-003 R2.3. Would very short term delegations (less than 30 days) for vacation and out-of-office travel need same level of recording and Senior Manager approval. 6) In this Standard and throughout several other CIP Standards, the lead focus statement in the Measures is re-stated redundantly throughout each of the bulleted Measure statements. Please

Organization	Yes or No	Question 2 Comment
		clean-up such text.
Response: 1) The addition of the "implement" language was in response to a determination in the FERC Order. [Please refer to FERC Order 706 Paragraph 75.] 2) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 3) The SDT believes that R2.3 provides Responsible Entities the flexibility to meet the leadership requirements without prescribing organizational changes. 4) Thank you for your comment. 5) There is no adjustment of the requirement based upon longevity of absence. 6) This modification was done in order to be in line with the structure of other ERO standards.		
Dynegy	No	Agree with proposed modifications except recommend moving CIP-003, R2 into the CIP-002 Standard (see comment on Item #1).
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Illinois Municipal Electric Agency	No	IMEA agrees with the intent of the proposed modifications, but recommends they be incorporated into CIP-002-1 (instead of CIP-003-1) modifications for clarification of applicability regardless of Critical Cyber Asset identification.
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for		

Organization	Yes or No	Question 2 Comment
a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Northern Indiana Public Service Company	No	As stated in question 1 I believe the revised applicability in CIP-003-2 section 4.2.3 is oddly placed as an entity could read CIP-002-2 in entirety and feel that the resulting null asset list excludes the entity from any other CIP standards. If a single requirement also applies to an entity that has a resulting null list, I believe it is better to call out the additional requirement within CIP-002-2 R4 rather than adding revised applicability language to CIP-003-2.
Response: The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Ontario IESO	No	With respect to individual bullet points: (1) We find this question confusing. We interpret Applicability as written to mean that those Responsible Entities that have determined that they have no Critical Cyber Assets need only to meet R2 of CIP-003. The question as posted here seems to suggest that R2 of CIP-003 only applies to these Responsible Entities, but NOT to those other Responsible Entities that have identified that they have Critical Cyber Assets. Please clarify. Currently, only CIP-002 is applicable to entities without Critical Assets. Thus, the recommended modification to CIP-003 would be insufficient for accomplishing the intent of the change. One solution might be to move the Senior Manager appointment requirement from CIP-003 R2 to CIP-002 (as suggested under Q1), or incorporate the requirement for a Senior Manager appointment by reference within CIP-002. (2) Agreed, and this is consistent with our comments on CIP-002, above. (3) Agreed (4) Agreed (5) Agreed
Response: To clarify, the question refers to the addition of a requirement for entities with no Critical Cyber Assets, not the exclusive application of CIP-003-2 R2 to entities with no Critical Cyber Assets. All Responsible Entities, regardless of their ownership of critical assets, are required to meet		

Organization	Yes or No	Question 2 Comment
CIP-003-2 R2. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Standards Review Committee of ISO/RTO Council	Yes No	(1) We are confused by the question asked here. We interpret Applicability as written to mean that those Responsible Entities that have determined that they have no Critical Cyber Assets need only to meet R2 of CIP-003. The question as posted here seems to suggest that R2 of CIP-003 only applies to these Responsible Entities, but NOT to those other Responsible Entities that have identified that they have Critical Cyber Assets. Please clarify. Currently, only CIP-002 is applicable to entities without Critical Assets. Thus, the recommended modification to CIP-003 would be insufficient for accomplishing the intent of the change. One solution might be to move the Senior Manager appointment requirement from CIP-003 R2 to CIP-002 (as suggested under Q1), or incorporate the requirement for a Senior Manager appointment by reference within CIP-002. Specific to R2, notwithstanding the above recommendation to move it to CIP-002, we have concerns with the inclusion of the words "single" and "authority." These inclusions present a specific example where the CIP Standards are overly prescriptive in that they seek to regulate company's internal management, as opposed to regulating performance. This modification is inappropriate, unnecessary and outside NERC's legislative mandate. The drafting team must explain what it intends by adding the word "authority" to the word "responsibility." Second, if "authority" is given a meaning of having the power to ensure that capital resources are expended to achieve the objectives laid out in the Standard, we have questions about how NERC can propose regulating how companies manage their budgets. Some companies budgets must be approved by their Boards, and some companies' budgets must be approved by FERC. (2) Agreed, and this is consistent with our comments on CIP-002, above. (3) Agreed (4) Agreed (5) Agreed
Response: To clarify, the question refers to the addition of a requirement for entities with no Critical Cyber Assets, not the exclusive application of CIP-003-		

Organization	Yes or No	Question 2 Comment
2 R2 to entities with no Critical Cyber Assets. All Responsible Entities, regardless of their ownership of critical assets, are required to meet CIP-003-2 R2. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Brazos Electric Power Cooperative, Inc.	No	Under the Applicability section it makes no sense for a Responsible Entity to have to comply with CIP003 R2 when there are no CCAs. This should be deleted.
Response: The intent of the application of CIP-003-2 R2 to Responsible Entities with no Critical Cyber Assets is to ensure that the appropriate individual approves the null list of Critical Cyber Assets.		
US Bureau of Reclamation	No	The reference to a senior manager in paragraph 381 was not intended be a requirement. FERC did allow registered entities some flexibility, to wit: "The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve". The modification by the SDT, which specifies delegation by the "senior manager", is intrusive upon the Responsible Entity's organizational structure. It is sufficient to require that the Responsible Entity must be able to produce documentation of who has responsibility for the CIP implementation. For geographically diverse organizations, that responsibility will change depending on the location of the affected systems. Each Responsible Entity generally has identified an individual who is authorized to submit documentation in response to a Regional Entity's requests or through the certification process. The specific requirement that the senior manager have the authority of leading and managing CIP is not the same as requiring certification and may not fit with the organizational lines of the Responsible Entity. Organizational structures must not be legislated in industry standards, especially when the organizations have a vast array of responsibilities and authorities that govern their function. Reclamation has functional responsibilities delegated to Regional Directors in order to manage the vast array of legislated mandates. To require Reclamation to alter its organizational structure in no way improves the reliability of the BES and the requirement appears arbitratry. Each entity certifies that it complies with the integrity of its security through one individual who is authorized to speak for the agency. The requirements should focus on the desired performance outcome which is needed to maintain reliability of the power system, not how the performance is accomplished.

Organization	Yes or No	Question 2 Comment
Response: The SDT believes that R2.3 provides Responsible Entities the flexibility to meet the leadership requirements without prescribing organizational changes.		
City of Tallahassee (TAL)	Yes	Although the "acceptance of risk" ties in with the discusson above on business judgement.
Response: The removal of “reasonable business judgment” was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: “Responsible Entity” is defined within the Applicability section of each CIP standard. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Suggest R3.1 read thirty calendar days.
Response: 1. NERC and Regional Entity are defined in NERC’s corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws. 2. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives		

Organization	Yes or No	Question 2 Comment
included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Pepco Holdings, Inc - Affiliates	Yes	We support the proposed modifications including the removal of business phone and business address from B. Requirements, R2.1. Similary, should the business phone requirement be removed from B. Requirements, R5.1.1 - Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-003-2, D. Compliance, Section 1.5 say "None"?
Response: Thank you for identifying the inconsistency. Section 1.5 should state, “None”, and “Business phone” in R5.1.1 will be removed.		
Ameren	Yes	None.
Response: Thank you for your comment.		
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Bonneville Power Administration	Yes	
Consumers Energy Company	Yes	
CoreTrace	Yes	

Organization	Yes or No	Question 2 Comment
Deloitte & Touche, LLP	Yes	
Detroit Edison Company	Yes	
Exelon	Yes	
FirstEnergy Corp	Yes	
Luminant Power	Yes	
Old Dominion Electric Cooperative	Yes	
Oncor Electric Delivery LLC	Yes	
PPL Corporation	Yes	
Progress Energy	Yes	
San Diego Gas and Electric Co.	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
WECC Reliability Coordination	Yes	

3. The The CSO706 SDT is proposing the following modifications to **CIP-004-1**:
    - In R1 and R2, clarify the requirement to implement security awareness and annual cyber security training programs.
    - Revise R2.1 to train personnel prior to granting access (per FERC Order, paragraph 431).
    - Revise R3 to complete a personnel risk assessment prior to granting access (per FERC Order, paragraph 443).
    - In Requirements R2.1 and R3, the SDT adopted the FERC Order 706 language, "except in specified circumstances such as an emergency," to address unusual events that demand urgent action before the personnel risk assessment can be completed.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

The majority of the comments were related to the requirement that a personnel risk assessment and requiste training must be completed prior to allowing personnel unescorted access to critical assets and critical cyber assets. Specific circumstances can be defined when unescorted access to the critical assets and critical cyber assets is permitted prior to completion of the personnel risk assessment and training, such as emergencies. Escorted access to protected areas is permitted, however, the escort must be 'continuous', that is an active process of escorting, and not passive, that is just being present in the same area (i.e., escorted).

Many of the commenters expressed concern over the definition of the "specific circumstances" under which unescorted access to the protected areas can be permitted, and they are looking for guidance. The SDT clarified that the responsible entity shall define its own specified circumstances and document them within the cyber security training program, personnel risk assessment program, or cyber security policy.

Several commenters expressed concern that elimination of the 30-day temporary unescorted access criteria may have an operational impact, since the personnel risk assessments and requiste training could take much longer to complete. The SDT restated that personnel can be granted such access as long as a personnel risk assessment has been conducted within the last seven years, and the minimum training has been conducted according to personnel roles and responsibilities.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT made the following changes to CIP-004-2 based on stakeholder comments:

R1. Awareness — The Responsible Entity shall establish, document, implement, and, maintain ~~document and implement~~ a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

R2. Training — The Responsible Entity shall establish, document, implement, and maintain ~~document and implement~~ an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, ~~reviewed~~ and shall be updated ~~as~~ whenever necessary.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

Organization	Yes or No	Question 3 Comment
Alberta Electric System Operator	No	The term "specified circumstances" implies that a set of circumstances is specified somewhere. Where is this list and who will decide what comprises it? Suggest that this list be clarified.
Response: This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.		
Consolidated Edison Company of New York, Inc.	No	CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
Response: This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.		
Detroit Edison Company	No	The language "except in specified circumstances such as emergency." introduces ambiguity into this requirement. What would other circumstances be? Is each Responsible Entity allowed to define this on their own? Paragraph 443 of FERC order 706 directs the SDT to provide guidance on defining

Organization	Yes or No	Question 3 Comment
		emergencies. "The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process."
Response: This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.		
Encari	No	1. The new language within R2.1 allows for an exception in specific circumstances. What are specified circumstances? And, if these specific circumstances occur do the individuals ever have to take the training? – The prior requirement was within ninety calendar days. 2. An additional crossover requirement exists leading to confusion. CIP-006-2 R3 now states cyber assets residing in a PSP; however the language now in CIP-004-2 does not require access to Cyber Assets to undergo training, awareness and PRAs. We recommend providing further clarification around this requirement.— General Comments Pertaining to All Standards–Other modifications were also made to this standard that are not included as part of the question. 3. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: 1. This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances. 2. If personnel roles and responsibilities require access after the specified circumstance, then training must be completed according to CIP-004. Personnel can be granted such access as long as a personnel risk assessment has been conducted according to the requirements in R3, and the minimum training has been conducted according to personnel roles and responsibilities according to the requirements in R2. 3. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting		

Organization	Yes or No	Question 3 Comment
		teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority. The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator, and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.
FirstEnergy Corp	No	Regarding R2.1 and R3, we believe that the phrase "specified circumstances such as an emergency" is ambiguous. It is not clear what would constitute acceptable "specified circumstances" other than an emergency situation. This phrase should be replaced with simply "emergency situations", which would also be consistant with language in other CIP requirements such as in CIP-003 R1.1.
Response: This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.		
Northern Indiana Public Service Company	No	Clarification regarding the definition of specified circumstances and emergency conditions is needed. Additionally, language needs to be added to clarify what steps need to be taken if an emergency occurs and access is granted. As the draft reads, an entity could declare an emergency, grant access, and document the emergency condition. There is no language directing follow up action that would ever require the responsible entity to perform training or a PRA of the individual that was granted access under the emergency condition. Depending on the direction provided from the drafting team in regards to what would consist of an emergency, the removal of the 30-90 day after the fact language may create significant concern in regards to bargaining unit operations and service personnel. Secondly, I have a comment regarding the additional clarifying language that was added to CIP004-2 R1 to indicate applicability to critical cyber assets. I understand that this language was added to provide uniformity in scope between CIP-004-2 R1, R2, and all of the respective sub-requirements. I have a concern regarding the absence of the CCA language in CIP-004-2 R3. I feel R3 should be modified to include similar CCA language to provide uniformity with R1, R2 and the R3 sub-requirements.

Organization	Yes or No	Question 3 Comment
Response: This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances. If personnel roles and responsibilities require access after the specified circumstance, then training and a personnel risk assessment must be conducted according to CIP-004. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Orange and Rockland Utilities Inc.	No	CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
Response: This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.		
Ameren	No	The elimination of the 30 day temporary access time will have a significant "operational" impact to fill personnel positions in a timely manner within protected areas. Without the 30 day temporary access criteria, personnel will not be allowed "unescorted" access into a facility until the candidate has completed training and a background check is completed, reviewed and returned with a positive and acceptable response. Additionally, mandating that another employee watch or "escort" the new candidate all the time during their shift is both a nuisance and a possible safety hazard. It is important to note that this proposed change is a "180 degree conceptual change" from what was a noticeable and unwavering stance that most companies took when the original CIP standards were implemented. Not being able to shift personnel around from one area of the company to the protected-area assignments (when personnel are re-assigned) immediately, places an unnecessary burden on both areas of the company. When comparing the proposed change to the current process, the benefits gained by the elimination of the 30-day temporary access window clearly don't outweigh what is already a solid and workable solution.

Organization	Yes or No	Question 3 Comment
Response: It has been identified in FERC Order 706 and the SDT agrees that the personnel risk assessment and requisite training shall be completed prior to granting unescorted access. Providing escorted access is permitted prior to the personnel risk assessment and requisite training being completed. Granting unescorted access is permitted for specified circumstances such as an emergency prior to the personnel risk assessment and requisite training being completed. The responsible entity shall define their own specified circumstances and document them within their cyber security training program, personnel risk assessment program, or cyber security policy.		
Tampa Electric Company	No	Requirement R3 The proposed changes would result in the language: "….A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency."(removing within 30 days of being granted access). This would leave the standard open to the interpretation that as long as an assessment is no older than 7 years old, then this risk assessment is "prior" to the personnel begin granted access. Tampa Electric is unsure if this is the intention of the language change. If this is not the intenct, then the wording should be clarified. Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: As stated in R3, personnel can be granted such access as long as the personnel risk assessment has been conducted within the last seven years. CIP-003-2 Requirement R3 includes the identification and approval of exceptions to the corporate Cyber Security Policy. Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.		
ISO New England Inc	No	1 – In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is edundant and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice.
Response: The word 'implement' was included per FERC Order 706 Paragraph 75 to remove any doubt that a particular process/procedure/program could		

Organization	Yes or No	Question 3 Comment
be only designed, developed, documented but not implemented. This was a result of previous questions around implementation from Industry. It is added for clarity and completeness.		
Standards Review Committee of ISO/RTO Council	No	In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundant and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice.
Response: The word 'implement' was included per FERC Order 706 Paragraph 75 to remove any doubt that a particular process/procedure/program could be only designed, developed, documented but not implemented. This was a result of previous questions around implementation from Industry. It is added for clarity and completeness.		
Applied Control Solutions, LLC	No	Training needs to be specifically control system cyber security training
Response: R2.2 defines minimum required items which are Critical Cyber Asset specific.		
San Diego Gas and Electric Co.	No	To help clarify training requirements for different users and access levels, SDG&E would like to see language added to CIP-004-1 R2.2 stating that training should be appropriate to user duties, functions, experience, and access level. Information concerning vulnerabilities should be revealed on a need to know basis and not universally.
Response: Given the limited scope and timeline for Phase 1, please re-address this issue during the Phase 2 comment period.		
US Bureau of Reclamation	No	Requirement R2 needs to more specifically distinguish between access types and required training. Individuals with physical access may only need general security awareness training, whereas those with physical and logical access may require specific role-based training. The requirement, as written, addresses proper use of cyber assets, physical and logical access controls, proper handling of information, etc., in what appears to be an all-inclusive manner. Some of these training requirements would appear to be unnecessary for an individual who may only need limited physical access and the requirement should support this. The requirement does not recognize that Entities may have a more rigorous background check process which takes longer than the abbreviated process described in the standard. While describing the minimum helps to clarify what is needed, the standard should allow Entities that have more rigorous requirements longer time frames to implement the background checks.

Organization	Yes or No	Question 3 Comment
		In most cases the background checks timeframes are not within the control of the Entity. In addition the standard would hamper the ability of existing experienced staff who have passed a more exhaustive check from operating thereby defeating the value to reliability. Can the requirement, R3, be structured in such a manner as to support access following initial screening in situations where full investigations may take a significant period of time? As an example, a national security check resulting in a clearance may take an extended period of time, limiting an organization's ability to utilize an employee - even in a decreased sensitivity role - while awaiting results. If the employee is allowed access - even limited - following a preliminary check (through local/national law enforcement agencies), would this meet the intent of the requirements while awaiting the results of a full and more comprehensive investigation? Further, is there a means, within the present requirements, to address the temporary "grandfathering" of individuals who have access today while they are undergoing investigations? Without such an allowance, staff availability, during investigation activities, could be severely limited.
Response: Personnel can be granted such access as long as a personnel risk assessment has been conducted according to the requirements in R3, and the minimum training has been conducted according to personnel roles and responsibilities, in accordance with the requirements in R2. A national security investigation contains elements beyond the scope of R3, which are not necessary to meet R3. As stated in R3, personnel can be granted access as long as the personnel risk assessment has been conducted within the last seven years. If a personnel risk assessment has not been conducted within the last seven years, it must be completed before the individual can be granted access.		
WECC Reliability Coordination	No	do not agree with R1.2 that personnel need to be trained before they are granted access. Training in this area is extensive and we feel the 90 day window allows appropriate training to take place along with our employee orientation.
Response: It has been identified in FERC Order 706 and the SDT agrees that the requisite training shall be completed prior to granting unescorted access. Providing escorted access is permitted prior to the requisite training being completed. Granting unescorted access is permitted for specified circumstances such as an emergency prior to the requisite training being completed. The responsible entity shall define their own specified circumstances and document them within their cyber security training program or cyber security policy.		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: “Responsible Entity” is defined within the Applicability section of each CIP standard. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this		

Organization	Yes or No	Question 3 Comment
concept. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Suggest rewording Requirement R2.1 as follows: “This program will ensure that all personnel requiring access to Critical Cyber Assets," for clarity.
Response: 1. NERC and Regional Entity are defined in NERC’s corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws. 2. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Southern Company	Yes	CIP-004 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-004 Section D - Compliance: 1.4.2 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-004 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC’s Rules of Procedure, Paragraphs 404 and 405). 1.4.2 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C –		

Organization	Yes or No	Question 3 Comment
Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT. 1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.		
Progress Energy	Yes	CIP004R2 – The cyber security training program shall be annually reviewed and updated as necessary – Please provide clarification, does updated as necessary mean updates only need to occur annually during the annual review period?
Response: The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary (e.g., due to system changes or reference material changes that are included as part of the training program that require changes in the training).		
Pepco Holdings, Inc - Affiliates	Yes	We agree with the proposed modifications especially with the phrase "except in specified circumstances such as an emergency". Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-004-2, D. Compliance, Section 1.5 say "None"?
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Deloitte & Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal training and awareness program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: Reliability standards are limited to specifying what to do, not how to do it. Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.		

Organization	Yes or No	Question 3 Comment
American Transmission Company	Yes	
Austin Energy	Yes	
Bonneville Power Administration	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
City of Tallahassee (TAL)	Yes	
Consumers Energy Company	Yes	
CoreTrace	Yes	
Duke Energy	Yes	
Dynegy	Yes	
Exelon	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
Manitoba Hydro	Yes	
MidAmerican Energy Company	Yes	

Organization	Yes or No	Question 3 Comment
MRO NERC Standards Review Subcommittee	Yes	
Northeast Power Coordinating Council	Yes	
Old Dominion Electric Cooperative	Yes	
Oncor Electric Delivery LLC	Yes	
Ontario IESO	Yes	
PacifiCorp	Yes	
PPL Corporation	Yes	
Southern California Edison Company	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
Xcel Energy	Yes	

4. The CSO706 SDT is proposing the following modifications to **CIP-005-1**:

   - In R1.5, clarify the requirement to safeguard Cyber Assets used in the control or monitoring of Electronic Security Perimeter.
   - The term "implement" was added to CIP-005-1 Requirement R2.3 to clarify that the procedure for securing dial-up access to the Electronic Security Perimeter must be both maintained and implemented.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

Most of the commenters agreed with these suggested changes to the standards.

The scope of the modification to the standards was clarified by the SDT to only include devices that perform access control and/or monitoring of the ESP as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT made the following changes to CIP-005-1 based on stakeholder comments:

R2.3. The Responsible Entity shall implement and maintain ~~and implement~~ a procedure for securing dial-up access to the Electronic Security Perimeter(s).

Removed all references to "dated" from the lists of appropriate evidence in Measures M1 through M5.

Organization	Yes or No	Question 4 Comment
Consolidated Edison Company of New York, Inc.	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). The corresponding requirements do not state a requirement for a date: adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
Response: The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		

Organization	Yes or No	Question 4 Comment
ISO New England Inc	No	1) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. 2) R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.
Response: 1) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards. 2) The text will be changed to read “documentation”. The SDT has received numerous comments related to wording preferences. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Northeast Power Coordinating Council	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.
Response: The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Orange and Rockland Utilities Inc.	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
Response: The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Bonneville Power Administration	No	The revision to CIP-005-2 R1.5 referenced only CIP-006-2 R3. CIP-003 R3 requires that the organization identify the Physical Security Perimeter. In the original CIP-005-1 R1.5, the physical protections had to meet CIP-006-1 R2 and R3 which are now renumbered R4 and R5 in CIP-006-2.

Organization	Yes or No	Question 4 Comment
		This represents a major revision and a much less robust security in the physical protection requirements for cyber assets used for access control or monitoring of the Electronic Security Perimeter. To retain the original intent of CIP-005-1 R1.5, the requirement must include a reference to CIP-006-2 R3, R4, & R5.
Response: CIP-006-R3 requires placing the devices of CIP-005-2 R1.5 within a Physical Security Perimeter. Once a device is within a Physical Security Perimeter, physical control is automatically established, making these inclusions redundant.		
Encari	No	1. It is very important to define monitoring in the new context. Originally the cyber assets had to be used for the dual purpose of access control and monitoring. Now, simply a monitoring device is considered a cyber asset under this new language. We ask for an additional clarification around to what extent monitoring is covered, for example: a. The original monitoring cyber asset (device a) b. The cyber asset receiving alerts from the original device (device b) c. The cyber asset forwarding the alerts (device c) d. The cyber asset receiving the alerts (device d) The current language could be interpreted in a way that a blackberry receiving alerts is "monitoring" the ESP. General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: 1. The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 2. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission		

Organization	Yes or No	Question 4 Comment
		Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence. 3. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority. The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.
MidAmerican Energy Company	No	Comment: On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. MidAmerican believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.MEC proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems - Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.

Organization	Yes or No	Question 4 Comment
Response: The scope of the modification is only to include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
MRO NERC Standards Review Subcommittee	No	On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.The MRO NSRS proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems? Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.
Response: The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Northern Indiana Public Service Company	No	I would request a clarification on scope and depth of the devices to be included in the access control and/or monitoring. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or monitoring of the ESP. I am concerned with

Organization	Yes or No	Question 4 Comment
		the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP.
Response: The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Tampa Electric Company	No	In R1.5, the change from “and” to “and/or” could bring unintended devices into scope of this standard. The change should be clarified to say “access control of and/or monitoring access to of the Electronic Security Perimeter(s).” Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
Response: The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Situations where standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The TFE process will address the requirements for documenting, approving, and remediating the exception. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been		

Organization	Yes or No	Question 4 Comment
addressed.		
Ontario Power Generation	No	R1.5 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those which are used to access CCAs
Response: Requirements apply regardless of who performs the functions.		
PacifiCorp	No	Yes to the second bullet. No to the first bullet and other points.R1.1 - It is unclear what is meant by "externally connected". Does "connectivity" refer to logical or physical connectivity? Is "external" a reference to the ESP in question, or to the entity? Is it a reference to layer 3 (and above)? PacifiCorp recommends some clarifying language similar to the following: • Any device accessible via routable protocol (layer 3) from outside the ESP is an access point unless such traffic is already passing through and controlled (layer 3) by another CIP005 compliant access point. • Additionally, any device serving as an endpoint of an encrypted and/or encapsulated layer 3 (and above) tunnel (IPSEC, GRE, SSL-VPN, SSH, CIPE, etc..) which provides remote network connectivity to the ESP network and not merely application access to the host itself, and where the other endpoint is outside the ESP, is also an access point.? • Externally connected also includes devices accessible via modem or any form of wireless access point providing network connectivity to other devices within the ESP." • Externally connected does not include encrypted communication links where the end points are within the ESP.R1.3 - This should be eliminated. By definition, communication links between discrete ESPs are "out of scope" (CIP-005-2 4.2.2) Additionally, where such links are using routable protocols, the termination point would be a "communication end point" and thus covered by R1.1. This section provides no additional value.R1.5 references to CIP005.R2 and CIP005.R3 should be removed as these are not applicable to the access control and monitoring equipment which are not "Access points". Additionally, the proper security practices for these devices are covered under CIP007 R2-R9.R1.5 (continued) - The access control

Organization	Yes or No	Question 4 Comment
		and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as mobile devices. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. PacifiCorp believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting mobile devices used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.PAC proposes the following language: R3. Protection of Electronic Access Control Systems - Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for mobile devices, for which the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.
Response: These types of issues will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.		
US Bureau of Reclamation	No	The standard should be worded to be applicable for existing dial-up access or if dial-up access is added.
Response: The requirement applies to all dial-up access, both existing and future.		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.		
Southern Company	Yes	CIP-005 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-005 Section D - Compliance: 1.4.2- Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-005 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of

Organization	Yes or No	Question 4 Comment
		confidential information.
Response: 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405). 1.4.2 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT. 1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.		
Southern California Edison Company	Yes	Request clarification on the difference between "process" and "procedure."
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Exelon	Yes	We support all comments noted for CIP005 in this section with the recommendation to move the word implement before maintain in R2.3 so the sentence reads ?implement and maintain.? Reason for the recommendation is a control must be implemented before it can be maintained
Response: The SDT will make the appropriate change in R2.3 from "maintain and implement" to "implement and maintain".		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.

Organization	Yes or No	Question 4 Comment
Response: "Responsible Entity" is defined within the Applicability section of each CIP standard. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Alberta Electric System Operator	Yes	
Ameren	Yes	
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
City of Tallahassee (TAL)	Yes	
Consumers Energy Company	Yes	

Organization	Yes or No	Question 4 Comment
CoreTrace	Yes	
Deloitte & Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e., a documentation of a formal dial-up security program and procedure that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: Reliability standards are limited to specifying what to do, not how to do it. Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.		
Detroit Edison Company	Yes	
Duke Energy	Yes	
Dynegy	Yes	
FirstEnergy Corp	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
Manitoba Hydro	Yes	
Oncor Electric Delivery LLC	Yes	
Ontario IESO	Yes	

Organization	Yes or No	Question 4 Comment
Pepco Holdings, Inc - Affiliates	Yes	
PPL Corporation	Yes	
Progress Energy	Yes	
San Diego Gas and Electric Co.	Yes	
Standards Review Committee of ISO/RTO Council	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
WECC Reliability Coordination	Yes	
Xcel Energy	Yes	

5. The CSO706 SDT is proposing the following modifications to **CIP-006-1**:

   - Clarify Requirement R1 that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. CIP-006-1 Requirements R1.1 through R1.7 and R1.9 were revised to clarify the elements that, at a minimum, must be addressed in the physical security plan.
   - The SDT added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2.
   - The SDT added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter.
   - Subsequent Requirements were renumbered and references were appropriately revised. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to lists of options consistent with the intent of the requirements.
   - The SDT revised the Measures to add "implementation" to Measure M1 documentation elements for Requirement R1, added Measure M2 to document the protection of physical access control systems, added Measure M3 to document the protection of electronic access control systems, and renumbered subsequent Measures and references to Requirements. The SDT also added failure to implement the security plan as Level 4 non-compliance.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

A significant number of the stakehoders submitted comments concerning which devices must be included in the Physical Security Plan. The SDT clarified that any device that is within the same electronic security perimeter as a critical cyber asset must be addressed in the Physical Security Plan.

The SDT also clarified that monitoring systems that do not authenticate and/or grant physical access are excluded from the CIP-006 R2 requirement.

A number of stakeholders expressed concerns about the reduction in the amount of time allowed for making changes and updates to the physical security plan from 90 days to 30 days. The SDT clarified that this change was made to achieve consistency in the documentation requirements across all of the CIP standards.

Many of the stakeholders raised a concern about meaning of the requirement for a 'continuous' escort for individuals that have not completed the personnel risk assessment and the requisite training for unescorted access. The SDT clarified that escorted

access to protected areas is permitted, however, the escort must be 'continuous', that is an active process of escorting, and not passive, that is just being present in the same area (i.e., escorted).

Some of the commenters raised concerns over the time period for data retention requirements as well as the confidentiality of the data. The SDT clarified that with the exception of retaining evidence in support of an investigation, the CIP standards define a finite data retention period. The Compliance Enforcement Authority may direct the Responsible Entity to retain evidence for a longer period of time as part of an investigation (refer to ERO Rules of Procedure. Reference the ERO Rules of Procedure). The data retention language in the CIP standards supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of the data. The audit data retention period is determined by the audit period for each Registered Entity.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT made the following changes to CIP-006-2 based on stakeholder comments:

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain~~, and implement~~ a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.2 Identification of all "physical" access points

R1.4. Appropriate use of physical access controls as described in Requirement ~~R3~~ R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

Organization	Yes or No	Question 5 Comment
Ontario IESO	No	With respect to individual bullet points: (i) R1: The reference to the Senior Manager should also refer to CIP-003 R2 to clarify the requirement. (ii) CIP-006 R1.6 should not require "continuous" escorted access, since demonstrating compliance with such requirement would be impossible. As an alternative, wording might indicate that visitors are to be escorted in a manner that ensures their actions can be supervised and unauthorized disclosures prevented, and/or only authorized employees can be escorts. (iii) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" (iv) R1.4, reference to R3 should read R4.

Organization	Yes or No	Question 5 Comment
Response: (i) The drafting team feels it made this distinction by the change from “a Senior Manager” to “the Senior Manager”. (ii) The drafting team feels that ‘continuous’ is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted). (iii) The drafting team feels the statement is clear that the access points are “physical” since the requirement is directed at Physical Security Perimeters; however the drafting team will implement this change. (iv) The drafting team agrees and will implement this change.		
US Bureau of Reclamation	No	The requirement that the Physical Security plan be approved by a single senior manager is not appropriate. It should be sufficient to require that the entity have a management approved plan. As stated before, submissions from the regional entities in geographically diverse entities pass through and are certified by the entity's compliance POC and represent an official entity position and commitment to action. To require more adds an unnecessary organizational and administrative burden.
Response: The requirement specifically provides for the Senior Manager or delegate(s) to approve the plan, thereby providing enough flexibility while maintaining a specific chain of authority.		
Southern California Edison Company	No	For R1.8 Annual review and approval - we interpret it as the Senior Manager or delegate reviews and approves the physical security plan annually. For consistency with R2, suggest re-wording R3 to: "Protection of Electronic Access Control Systems - Cyber Assets that authorize and/or log access to the Electronic Security Perimeter (s) shall reside within an identified Physical Security Perimeter." Delete R2.1.
Response: The drafting team feels that since Requirement 1.8 is a subrequirement of Requirement 1, it is appropriate to interpret that the annual review would be signed off by the senior manager or delegate as identified in Requirement 1. For your additional comments, these types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.		
Standards Review	No	(i) R1: We recommend revising "the Senior manager" to "a senior manager" as the requirement should

Organization	Yes or No	Question 5 Comment
Committee of ISO/RTO Council		not be job title specific. Further, the reference to "a Senior Manager" also should be made to CIP-003 R2 to clarify the requirement. (ii) CIP-006 R1.6 should not require "continuous" escorted access, insofar as that would create a condition that is impossible to prove to auditors. As an alternative, wording might indicate that visitors are to be escorted in a manner to ensure their actions can be supervised and unauthorized disclosures prevented, and/or only authorized employees can be escorts. (iii) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" (iv) R1.4, reference to R3 should read R4.
Response: (i) The drafting team feels it made this distinction by the change from “a Senior Manager” to “the Senior Manager”. (ii) The drafting team feels that ‘continuous’ is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted). (iii) The drafting team feels the statement is clear that the access points are “physical” since the requirement is directed at Physical Security Perimeters; however the drafting team will implement this change. (iv) The drafting team agrees and will implement this change.		
CenterPoint Energy	No	An additional modification that was proposed by the SDT in R1.7 reduced the amount of time allowed for making changes and updates to the physical security plan from 90 days to 30 days. CenterPoint Energy strongly disagrees with this change. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any physical security plan changes.

Organization	Yes or No	Question 5 Comment
Response: (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Xcel Energy	No	Xcel Energy feels strongly that 30 days is too short of a time frame to get drawings updated, Sr. Management approval,..etc. every time there is a change to the plan. We feel that 60 calendar days is more attainable industry-wide.
Response: (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Tampa Electric Company	No	Requirement 1.3: Remove "processes" from the wording to be consistent with the other changes in CIP006 Requirement 1 and eliminate the redundancy of having "processes" and "procedures" in same statement. Processes are included in the procedures. Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been		

Organization	Yes or No	Question 5 Comment
addressed. Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.		
Consolidated Edison Company of New York, Inc.	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any": a change generally includes more processes than just the change, e.g. acceptance period, required internal approvals, "as built" regulatory approvals.
Response: 1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters; however the drafting team will implement this change. 2) The drafting team agrees and will implement this change. 3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted). 4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Dynegy	No	1. Recommend changing R1.2 to require identification of all "physical" access points. 2. Correct R1.4 to reference R4 instead of R3. 3. Eliminate "continuous" from R1.6. This term is not auditable.

Organization	Yes or No	Question 5 Comment
Response: 1. Adding “physical” to access point in R1.2 - the drafting team feels that it is clear that the access points are “physical” since the requirement is directed at Physical Security Perimeters; however the drafting team will implement this change. 2. The drafting team agrees and will implement this change. 3. The drafting team feels that ‘continuous’ is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).		
ISO New England Inc	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous." it is subjective and will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar daysof the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"
Response: **1)** Adding “physical” to access point in R1.2 - the drafting team feels that it is clear that the access points are “physical” since the requirement is directed at Physical Security Perimeters; however the drafting team will implement this change. 2) The drafting team agrees and will implement this change. 3) The drafting team feels that ‘continuous’ is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted). 4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Northeast Power Coordinating Council	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points". 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous", and that it will be difficult to

Organization	Yes or No	Question 5 Comment
		demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the entity's change process for any".
Response: **1)** Adding “physical” to access point in R1.2 - the drafting team feels that it is clear that the access points are “physical” since the requirement is directed at Physical Security Perimeters; however the drafting team will implement this change. 2) The drafting team agrees and will implement this change. 3) The drafting team feels that ‘continuous’ is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted). 4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Ontario Power Generation	No	Requirement R2.1 will limit the ability of entities to leverage existing personnel to perform such duties as allocating access cards to legitimate visitors. Such duties are frequently delegated to trained reception personnel. OPG believes that allowance must be made for workstations in reception areas and selected offices areas (e.g. Human Resources departments). Cyber controls such as dual authentication on the workstation would be sufficient to meet the protective needs of the system. As noted earlier with respect to CIP 005-2 R1.5, OPG believes that CIP-006-2 R3 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those which are used to access CCAs. With respect to R1.6 there is concern that the addition of the new word "continuous" it will be difficult to demonstrate compliance. Requirements need to be enforceable. We recommend removing "continuous". We are concerned with the change in R1.7 reducing the time to update the Physical Security Plan from 90 to 30 calendar days. In a large organization this timeframe may not be achievable.

Organization	Yes or No	Question 5 Comment
		Changes to CIP-006 R1.1 open up concerns about the protection of non- Critical Cyber Asset components such as cables. To eliminate this concern we request that the wording of the last sentence be returned to read "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets."
Response: Any device that has the ability to authorize and or log access to Physical Security Perimeters must be physically protected per requirement CIP-006-2 R2. Relating to your comment on CIP-006-2 R3, the Requirements apply regardless of who performs the functions. The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted). (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days. Requirement 1.1 specifically addresses Cyber Assets and not a subset of Critical Cyber Assets. Any device that is within the same Electronic Security Perimeter as a Critical Cyber Asset must be within a Physical Security Perimeter, and hence must be addressed within the Physical Security plan.		
Orange and Rockland Utilities Inc.	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"

Organization	Yes or No	Question 5 Comment
Response: 1) Adding “physical” to access point in R1.2 - the drafting team feels that it is clear that the access points are “physical” since the requirement is directed at Physical Security Perimeters; however the drafting team will implement this change.. 2) The drafting team agrees and will implement this change. 3) The drafting team feels that ‘continuous’ is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted). 4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
TVA	No	We agree with all except, CIP-006 R1.6. CIP-006 R1.6 requires a "continuous" escort. We agree that performing escort duties in a manner that ensures visitors actions are supervised and malicious attempts are prevented is critical. However, being able to provide auditable proof of "continuous" escorting creates a condition that is impossible to meet. We propose the following: R1.6: Policy and procedures describing roles, responsibilities, and corrective action in regard to escorting personnel not authorized for unescorted access within the Physical Security Perimeter. We would also recommend that Responsible Entitie obtain a signature for record from individuals performing escort duties demonstrating that they acknowledge and accept their role and responsibilities and understand what corrective actions will be taken for any breach in procedure.
Response: The drafting team feels that ‘continuous’ is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).		
Austin Energy	No	The original stated intent of the Standards was to protect against 'cyber' attacks. Modifications to R2 would seem to overstep the intent in the case where a separate non-critical system was used the monitor assess to Critical Cyber Assets (CCA). Now if the CCA was itself incorporated into the physical assess monitoring then the modification to R2 is self evident. However, when a separate system is employed, it takes a coordinated effort by humans with a physical presence to pull off an attack. Although this may certainly qualify as espionage, there is nothing 'cyber' about it. It is proposed that an exception be made for cases where a separate system is used to monitor CCA.

Organization	Yes or No	Question 5 Comment
Response: The original standards were to protect the Cyber Assets from both cyber and physical attacks. While most of the standards deal with cyber protections, the easiest method to successfully attack a cyber asset is through physical means. The modifications in CIP-006 clarify cyber protections afforded to the systems that assist in the physical protection, including access and monitoring. Monitoring systems that do not authenticate and/or grant physical access are excluded from this requirement. An example would be a CCTV system that performs the monitoring role and also supports access logging, but does not control the Physical Security Perimeter access point.		
Bonneville Power Administration	No	While the majority of the revisions to R1 do provide clarity, the revision to Requirement R1.1 is less clear than the previous version and represents a change to the requirement. In the previous version, R1.1 requires that the Physical Security Plan address "Processes to ensure and document that" all Cyber Assets within an Electronic Security Perimeter reside within an identified Physical Security Perimeter consisting of a six-wall border. With this new revision, the Physical Security Plan shall address all Cyber Assets within an Electronic Security Perimeter. Address cyber assets how? There is no longer any requirement to describe the process the organization uses to ensure that cyber assets reside within an identified Physical Security Perimeter. Is the intent of this revision to clarify that a Physical Security Plan must simply exist and address identified Physical Security Perimeters protecting Cyber Assets within an Electronic Security Perimeter? There is no requirement for Physical Security Plans for cyber assets used for access control and/or monitoring of Physical Security Perimeters or Electronic Security Perimeters. If the intent of Phase 1 changes to R1 are simply to provide clarity, then recommend retaining the original R1.1 text from the previous version and make changes to R1.1 in a later phase of Project 2008-06 - Cyber Security Order 706.
Response: Requirement 1 identifies what must be within the Physical Security Plan, and Requirement 1.1 identifies that all cyber assets within an ESP must be within a Physical Security Perimeter, (i.e, the plan must address ensuring that all cyber assets within an ESP are within a PSP). Relating to exclusion of cyber assets used for access control and/or monitoring from the Physical Security Plan, the SDT refers you to Requirements 1.2 and 1.3.		
Brazos Electric Power Cooperative, Inc.	No	In R1.3, replace "the perimeter(s)" with "the Physical Security Perimeter(s)". In R8.3, need to clarify what "outage records" are. In M2, replace "shall make available documentation that" with "shall make available documentation showing how " In M3, replace "shall make available documentation that" with "shall make available documentation

Organization	Yes or No	Question 5 Comment
		showing how".
Response: The drafting team feels it is clear that the perimeters are “physical” since the requirement is directed at Physical Security Perimeters. Requirement 1.3 is a sub requirement of R1, “Physical Security Plan”. With respect to your comments on R8.3, M2, and M3 issues, these will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.		
Encari	No	1. The redlining appears to be inaccurate. For example R2 in CIP-006-1 is now R4 in CIP-006-2. This modification is very important to note as compliance monitoring systems may have been defined to key on the requirement field. 2. CIP-006-2 R4/R5/R6 now use bullets instead of numbered identifiers for the individual physical access methods. A unique identifier should be selected to identify these bulleted items. 3. R3 requires cyber assets used in the access control and/or monitoring of the ESP to be in a PSP. Please see our comments in Question 4 (CIP-005-2) pertaining to the extent of what assets need to be in a PSP (device a / b / c / d). – General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: 1. The drafting team agrees that not all of the changes are clearly identified. The posted version (the one that was commented on) is the official version, and while the drafting team did renumber some of the requirements, these are consistent across the reliability standards. 2. The changes that made individual sub-requirements into bullets were made to correct an original error, since requirements cannot be levied upon an item that may not be implemented. 3. CIP-006-R3 requires placing the devices of CIP-005-2 R1.5 within a Physical Security Perimeter. Once a device is within a Physical Security Perimeter, physical control is automatically established, making these inclusions redundant. Relating to not including all of the changes within the questions, the questions were meant to only address substantive changes to the standards. General: The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams		

Organization	Yes or No	Question 5 Comment
could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority. The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.		
MidAmerican Energy Company	No	See comment for question 5
Response: The scope of the modification is only to include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.The MRO NSRS proposes the following language:CIP-006 R3. Protection of Electronic Access Control Systems ? Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party. The MRO NSRS agrees with the remaining changes in CIP-006-2.

Organization	Yes or No	Question 5 Comment
Response: The intent of the modification was to clarify that a device that performs either function must be included. However an unintended consequence of this change was to add ambiguity as to what constitutes a monitoring device. The intent is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Northern Indiana Public Service Company	No	In future drafts I would encourage the drafting team to enable track changes on the modifications to the requirements numbers as well as the text. Modifications to requirement numbers, especially in CIP-006-2 were not consistently red-lined to display where the content was formerly referenced in the existing CIP-006-1. Regarding CIP-006-2 R2 I would request a clarification on scope and depth of the cyber assets that authorize and/or log access to the PSP. The previous language would have limited the devices to those that performed control and monitoring of the PSP (traditional physical access control security systems, and localized panels that communicate with the main system). The new language provided in the draft under CIP-006-2 R2 modifies the scope to include cyber assets that authorize and/or log access to the PSP. I am concerned with the depth of devices involved in the authorization or logging chain. Specifically: log correlation servers, backup and recovery servers, cameras, badge printing workstations, camera monitoring stations, log printers, etc. In the current draft it is unclear whether the device performing the authorization and/or logging is the only cyber asset that is subject to the requirements specified in CIP-006-2 R2.1-R2.2 or if all devices involved in authorization or logging are subject to those requirements specified in CIP-006-2 R2.1-R2.2. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets that authorize and/or log access to the PSP. Regarding CIP-006-2 R3 I reiterate my request for a clarification on scope and depth of the devices to be included in the access control and/or monitoring of the ESP. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or monitoring of the ESP. I am concerned with the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In

Organization	Yes or No	Question 5 Comment
		the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP. When providing the scope and depth clarification of these cyber assets, the drafting team needs to give consideration in regards to an entities ability to satisfy the new CIP-006-2 R3 requirements of containing all of the cyber assets used in the access control and/or monitoring within an identified PSP. In regards to CIP-006-2 R4-R6, I believe the sub requirement identifiers were removed as they are not specific requirements, but rather a means to satisfy the requirement. I believe the bullet items need some level of identifier for reference purpose. Potentially a B4.1, B4.2, etc. this would allow for an entity to reference the manner in which they satisfy the requirement.
Response: The drafting team agrees that not all of the changes were clearly identified. However, the posted version (the one that was commented on) is the official version, and while the drafting team did renumber some of the requirements, these are consistent across the reliability standards. In relation to your comments on CIP-006-2 R2 and R3, the intent of the modification was to clarify that a device that performs either function must be included. Monitoring systems that do not authenticate and/or grant physical access are excluded from this requirement. The intent is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. With respect to your comments on CIP-006-2 R4-R6, while the drafting team did renumber some of the requirements, these are consistent across reliability standards. The changes from individual sub-requirements to bullets were made to correct an original error where requirements cannot be levied upon an item that may not be implemented.		
PacifiCorp	No	No for the third bullet (R3) (See comment on CIP-005-2). Yes for remaining bullets.

Organization	Yes or No	Question 5 Comment
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
San Diego Gas and Electric Co.	No	SDG&E has the following comment to make about CIP-006-2 R2.1: This requirements states that cyber assets that authorize and/or log access to PSPs must be "protected from unauthorized physical access." In addition, R2.2 states that these cyber assets must be afforded the protective measures specified in, among others, CIP-006-2 R4, which addresses physical access control. Including both of these statements seems redundant. We recommend removing R2.1 and appending the text of R2.2 to R2 (thus allowing the deletion of R2.2)
Response: The SDT respectfully disagrees with the comment. The Reference in R2.2 to CIP-006-2, R4, defines the procedural and operational control requirements for the Physical Security Perimeter access points (e.g., doors with card access readers or other access authentication processes). R2.1 refers specifically to protecting the authorization and logging systems, recognizing that in some cases it is not practical to require that the systems reside within a defined Physical Security Perimeter.		
Manitoba Hydro	No	The wording in R2 should be: "Cyber Assets used in the access control and/or monitoring and/or logging access to the Physical Security Perimeter(s)", to reflect similar wording in R3, and to include other devices or systems used in access control, such as authentication systems.
Response: Issues such as clarifying the difference between logging and monitoring will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns were not addressed.		
Detroit Edison Company	No	CIP-006-2 R1.4 references "physical access controls as described in Requirement R3". R1.4 should reference Requirement R4 since the requirements were renumbered and Physical Access Controls is now R4.CIP-006-2 Introduction, 3. Purpose, it should read something like, ?. . . . . to ensure the implementation and continued maintenance of a physical . . . . . ? This program is not only being implemented, but will also be maintained going forward. (i.e. ? does not make sense to implement a program and do nothing else)CIP-006-2 Introduction, 4.2 The following are exempt from Standard CIP-006-2, in addition to listing the exemptions to NERC Standard CIP-006, they may also want to comment on potentially overlapping security requirements for facilities which are also regulated under the

Organization	Yes or No	Question 5 Comment
		Maritime Transportation Security Act (33 CFR 101/105) and the Chemical Facility Anti-Terrorism Standards. (6 CFR 27)CIP-006-2 R2 Protection of Physical Access Control Systems, sub-requirements R2.1 & R2.2. R2.1 is ambiguous in that it states, "Be protected from unauthorized physical access," yet it does not explain how this is to be accomplished. R2.2 defines the protective measures to be utilized? R4 and R5, Physical Access Controls and Monitoring Physical Access. It appears they want to grant the responsible entity flexibility in R2.1, but then it is limited by R2.2. These two sub-requirements should be combined into one to avoid confusion.
Response: The Drafting team agrees that R1.4 should reference R4 and not R3. This change will be implemented. With regard to inclusion of maintenance within the Purpose of the requirement, the drafting team agrees that this could add clarity however for consistency we would need to review how this would impact the purpose statements of the remaining CIP standards hence this will be addressed in Phase 2. The issue of conflicting regulatory authorities will be brought before NERC for discussion. Relating to protection of Physical Access Control Systems, reliability standards only prescribe "What" and not "How". These types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.		
Duke Energy	No	The language introduced in R2 and R3 has created an inconsistency with the use of the phrases "authorize and/or log access" and " access control and/or monitoring". This creates confusion and opportunity for differing interpretations of the requirements.
Response: Issues such as inconsistencies will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.		
PPL Corporation	No	Recommend a correction to R1.4 which references R3. We believe this is now R4.
Response: The drafting team agrees with the correction of Requirement 1.4, and will implement this.		
Alberta Electric System Operator	Yes	R1.1 is missing the word, "critical" for Cyber Assets. There is no need to have a requirement for assets that are not critical.
Response: Requirement 1.1 specifically addresses Cyber Assets and not the subset of Critical Cyber Assets. Any device that is within the same Electronic Security Perimeter as a Critical Cyber Asset must be within a Physical Security Perimeter and hence must be addressed within the Physical		

Organization	Yes or No	Question 5 Comment
Security plan.		
Exelon	Yes	(1) Recommendation to increase the timeframe in R1.7 to update the physical security plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation. (2) We support all the other comments noted for CIP006 in this section with the recommendation to move the word implement before maintain in R1 so the sentence reads "create, implement and maintain." Reason for the recommendation is a control must be implemented before it can be maintained.
Response: (1) (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days. (2) Revising the order of "create, implement, and maintain" is accepted.		
Progress Energy	Yes	CIP006R1.7 – We believe the reduction of 90 to 30 days for updates to the Physical Security Plan is inadequate when you consider the number and levels of approvals required to complete the updates. PE recommends leaving the 90 day time period.
Response: (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.

Organization	Yes or No	Question 5 Comment
Response: "Responsible Entity" is defined within the Applicability section of each CIP standard. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Requirement R1.4, it is not clear what is intended by the phrase "response to loss." 3) Requirement R1.4 should reference R4 rather than R3. 4) Suggest standardizing the language used in R4, R5 and R6. (R4 refers to security personnel; R5, second bullet, to authorized personnel; R6, third bullet, to security or other authorized personnel.)
Response: 1. NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws. 2. "Response to loss" in this requirement refers to loss of the visitor pass or physical access control method as described in R4. 3. The drafting team agrees with the correction of Requirement 1.4, and will implement this. **4.** Standardizing language will additionally be addressed in Phase 2.		
KEMA	Yes	In R4 and R6, access control and logging should include in and out of the Critical Facility in accordance to NERC's Security Guidelines for the Electricity Sector: Physical Security--Substations Dated 10-2004. Responsible entities should control and log in and out access to Critical Facilities to maintain a high level of access security to Critical Cyber Assets.
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives		

Organization	Yes or No	Question 5 Comment
included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Southern Company	Yes	CIP-006 R1.1 - Change to the last sentence should be clarifed that it applies to Critical Cyber Assets and not Critical Assets. R1.4 makes reference to "Requirement 3", but the correct reference in the new standard should now be "Requirement 5". CIP-006 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-006 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-006 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: Within CIP-006 R1.1, the requirement now reads “to such Cyber Assets”. The Drafting team agrees that the R1.4 reference is incorrect. The SDT points out that the correct reference is R4 and not R5. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC’s Rules of Procedure, Paragraphs 404 and 405). 1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT. 1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.		
Ameren	Yes	

Organization	Yes or No	Question 5 Comment
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
BC Transmission Corporation	Yes	
City of Tallahassee (TAL)	Yes	
Consumers Energy Company	Yes	
Deloitte & Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal physical security program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: Reliability standards are limited to specifying what to do, not how to do it. Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.		
FirstEnergy Corp	Yes	
Kansas City Power & Light	Yes	
Luminant Power	Yes	
Oncor Electric Delivery LLC	Yes	

Organization	Yes or No	Question 5 Comment
TransAlta Centralia Generation, LLC	Yes	
United Illuminating Company	Yes	
WECC Reliability Coordination	Yes	

6. The CSO706 SDT is proposing the following modifications to **CIP 007-1:**

   - Add "implement" to CIP-007-1 Requirements R2, R3 and R7 to clarify that processes and procedures must be implemented as well as documented.
   - Remove the "acceptance of risk" language (per FERC Order 706, paragraph 622) in Requirements R2.3, R3.2 and R4.1.
   - Revise the timeframe for documenting changes to systems or controls to thirty days in Requirement R9.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Many of the stakeholders raised concerns about the shortening of the documentation update period to 30 days following final implementation of changes to field equipment, systems, or processes. The SDT confirms the requirments for the 30 day period, especially since the update period begins upon final implementation of the changes. At that point, much of the due diligence should already have been completed related to the actual implementation with final documentation to follow within 30 days.

Many stakeholders expressed concerned about the removal of the "reasonable business judgment" language from the CIP standards. However, this was done in accordance with FERC Order 706. The definition of the Technical Feasibility Exception Process should address the concerns regarding the removal of the reasonable business judgment and acceptance of risk language from the standards.

A number of stakeholders raised concern about the new wording of the Purpose Statement for CIP-007 to include the phrase "other cyber assets". The SDT agreed to change the wording of the Purpose Statement to read "other (non-critical) Cyber Assets" as a way of clearing up the meaning and possible ambiguity. This is a similar structure to the wording used in the Implementation Plan for the CIP standards.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT made the following modification to the Purpose statement, based on stakeholder comments:

Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

Organization	Yes or No	Question 6 Comment
US Bureau of Reclamation	No	More rational is needed to explain the decision to remove "acceptance of risk" and "reasonable business judgement" language from CIP requirements while leaving the ability to identify "exceptions" through cyber security policy (CIP-003-2, R3.) With this exception in place, entities will be able to establish "policy" that will allow for deviation from the requirements outlined in the Standards. If the intent of the changes was to limit implementation disparity across all entities by removing "risk based decisions", the potential remains that an entity will establish exceptions through relaxed "policy" and the disparity will remain. If the intent was to remove any avenue for not meeting or implementing the requirements, entities may continue to accept "risk based decisions" (although not formally identified as such) by pursuing relaxed policy via exceptions (CIP-003-2 R3).Further, entities may have numerous "systems" of differing capabilities and generations. To require that exceptions be documented in "policy" does not acknowledge the diversity of systems that may be in service in an organization in as effective a manner as documenting exceptions as a function of the system, its environment, and its criticality. Such documentation would be better addressed through specific risk-acceptance decisions tied to specific systems, rather than to an all-encompassing "policy. "Finally, as CIP-003 is amended, entities may not implement or meet certain requirements, as long as, they are identified and documented as "policy exceptions." Was this the intent of the authors? We recommend that risk-managed approaches to cyber security requirements be reinstated into the requirements, recognizing that such a change will require FERC to reassess their order.
Response: The recommendation of using a risk-managed approach to cyber-security requirements is well appreciated and will be a significant topic in the next revision phase of the CIP Standards. The removal of “reasonable business judgment” was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.		
Consolidated Edison Company of New York, Inc.	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process." See comments to question 5.
Response: Since each entity’s change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not reliably drive the process for having documentation completed within thirty days of the actual modification to the systems or controls.		
Exelon	No	Recommendation to increase the timeframe in R9 to document changes to systems or controls to 60

Organization	Yes or No	Question 6 Comment
		days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.
Response: (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
ISO New England Inc	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
Response: Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not reliably drive the process for having documentation completed within thirty days of the actual modification to the systems or controls.		
Northeast Power Coordinating Council	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the entity's change process."
Response: Each entity's change process may be different and processes may include a number of steps to be performed after the actual change is completed over an extended period of time. The proposed wording will not reliably drive the process for having documentation completed within thirty days of the actual modification to the systems or controls.		
Ontario Power Generation	No	Reducing the timeframe for documenting changes to systems or controls in R9 from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.
Response: (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30		

Organization	Yes or No	Question 6 Comment
day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Orange and Rockland Utilities Inc.	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
Response: Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not reliably drive the process for having documentation completed within thirty days of the actual modification to the systems or controls.		
Southern California Edison Company	No	The change from 90 days to 30 days is difficult to achieve. SCE suggests 60 days to provide ample time for internal due diligence.
Response: (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
WECC Reliability Coordination	No	R2.3, R3.2 and R4.1 removes an organizations ability to accept minimal risk which cannot be compensated for.R9, we think 90 days is a reasonable time frame, 30 days is too restrictive.
Response: FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. For example, Responsible Entities should implement the requirements for ports and services for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to technical feasibility exceptions including reporting requirements and the implementation of compensating measures. The drafting team feels that one entity cannot accept risk for another entity in an interconnected power system. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process (Please refer to FERC Order 706, Paragraph 151). (FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an		

Organization	Yes or No	Question 6 Comment
operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Ameren	No	Acceptance of risk for certain ports and services is within security best practices. Mitigating controls for certain ports and services could effect the reliable operation of the bulk electric system.
Response: FERC directed the ERO to have a technical feasibility exception process supersede all instances of acceptance of risk. For example, Responsible Entities should implement the requirements for ports and services for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to technical feasibility exceptions including reporting requirements and the implementation of compensating measures. The drafting team feels that one entity cannot accept risk for another entity in an interconnected power system. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process (Please refer to FERC Order 706, Paragraph 151).		
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.		
Brazos Electric Power Cooperative, Inc.	No	1) In R5.1.1, replace "user accounts" with "user access privalges". 2) In R6.4, replace "all logs" with "all logs of system events related to cyber security". 3) In M2, replace "available documentation" with "available documentation of all ports and services".
Response: 1) All aspects of R5.1 are specific to individual and shared system accounts. User access privileges are covered in CIP-004. 2) The requirement is to retain all logs from all applicable cyber assets for 90 days. Log retention of system events related to cyber security		

Organization	Yes or No	Question 6 Comment
		may be longer based on incident response and reporting plan as defined by CIP-008. 3) The SDT reviewed and concluded that changing the wording as suggested would exclude the process documentation. It remains applicable to all documentation related to R2.
Encari	No	1. We recommend striking the following language from the Purpose section - "those systems determined to be Critical Cyber Asset, as well as the other". – General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Response:

1. The word “non-critical” will be added back into the purpose statement within parentheses beside the word other [i.e “other (non-critical)”], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity.
2. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity’s performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.
3. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.
4. The language of 1.4.2 indicates that the Compliance Enforcement Authority “in conjunction with” the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.

   The phrase, “in conjunction with” was deliberately used to recognize that there may be some confidential records that fall into the category of “critical energy infrastructure information” as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.

   The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission

Organization	Yes or No	Question 6 Comment
Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.		
MidAmerican Energy Company	No	Comment: MidAmerican does not agree with the change within the Purpose section of the standard to change the term ?non-critical? to ?other.? MEC proposes the following language Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
Response: The word "non-critical" will be put back into the purpose statement within parentheses beside the word other [i.e “other (non-critical)”], which is similar to the structure in the implementation plan. The additional wording is meant to remove ambiguity.		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS do not agree with the change within the Purpose section of the standard to change the term “non-critical” to “other.” The term "other" is too vague. The MRO NSRS proposes the following language: Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
Response: The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e “other (non-critical)”], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity.		
Northern Indiana Public Service Company	No	Within the purpose section of CIP-007-2 I would recommend the removal of the following language “those systems determined to be Critical Cyber Assets, as well as the non critical” as this language is redundant.
Response: The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e “other (non-critical)”], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity.		
CoreTrace	No	The modifications above are acceptable, however R4.2, as written, implies that all anti-virus and malware prevention tools have signatures, which is not true. Specifically whitelisting or behavioral

Organization	Yes or No	Question 6 Comment
		approaches do not require signature updates. Whitelisting in particular provides greater antivirus/antimalware protection than traditional signature based antivirus, including zero day protection, yet does NOT require “signatures”. Whitelisting relies on a positive security model that complements CIP 003 Configuration Control Requirements. By clarifying that traditional signature based antivirus is not required, NERC opens up the range of platforms and systems that can be protected greatly. For example, traditional antivirus does not exist for most Unix based systems, however whitelisting does. Propose revising R4.2 to read as follows: R4.2. If the Responsible Entity chooses to implement signature based antivirus or malware prevention tools the Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention ?signatures.? The process must address testing and installing the signatures. This requirement does not apply for non-signature based antivirus or malware prevention tools such as those based on whitelisting or behavioral analysis.
Response: R4.2 was not changed during this revision of the CIP Standards. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.		
PacifiCorp	No	Other comment: R5.3 - Instead of prescribing specific password construction standards, it would be better to express desired outcomes in terms of measurable entropy. The standards should require a certain level of protection against password guessing and brute force "hash cracking" attacks, but leave specifics to the implementers. For example, the standard could simply require 24 bits min-entropy per NIST Special Publication 800-63.
Response: R5.3 was not changed during this revision of the CIP standards. These types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.		
City of Tallahassee (TAL)	Yes	Although the "acceptance of risk" ties in with the discusson above on business judgement.
Response: The removal of “reasonable business judgment” was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.		
Duke Energy	Yes	Regarding R2.3, R3.2 and R4.1, we understand that the Responsible Entity's action to document compensating measures is sufficient to achieve compliance with the requirements, and that the

Organization	Yes or No	Question 6 Comment
		Responsible Entity does not need to also invoke the "Technical Feasibility" exception. Technical Feasibility is only applicable when the Responsible Entity cannot comply with a requirement. We also recommend that the Responsible Entity be required to perform an analysis of the residual risk after all compensating measures are applied. Add the words "and analysis of residual risk" to the end of R2.3, R3.2 and R4.1
Response: FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151] The Technical Feasibility Exception process is under development by NERC staff. Please readdress this issue during the Phase 2 comment period.		
Progress Energy	Yes	CIP007R9 – The reduction from 90 to 30 days is inadequate. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: “Responsible Entity” is defined within the Applicability section of each CIP standard. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Southern Company	Yes	CIP-007 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement

Organization	Yes or No	Question 6 Comment
		authority. CIP-007 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-007 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405). 1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT. 1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.		
Deloitte & Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e., a documentation of a formal security management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: Reliability standards are limited to specifying what to do, not how to do it. Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.		

Organization	Yes or No	Question 6 Comment
Alberta Electric System Operator	Yes	
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Bonneville Power Administration	Yes	
Consumers Energy Company	Yes	
Detroit Edison Company	Yes	
Dynegy	Yes	
FirstEnergy Corp	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
Manitoba Hydro	Yes	
Oncor Electric Delivery	Yes	

Organization	Yes or No	Question 6 Comment
LLC		
Ontario IESO	Yes	
PPL Corporation	Yes	We fully support the revisions in section B, Requirements.
Response: Thank you for your comment.		
San Diego Gas and Electric Co.	Yes	
Standards Review Committee of ISO/RTO Council	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
Xcel Energy	Yes	

7. The CSO706 SDT modified **CIP-008-1** Requirement R1 to clarify the requirement to implement the plan in response to cyber security incidents, update the plan within thirty days of any changes, and clarify that tests of the plan do not require removing components or systems during the test.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Many of the stakeholders disagreed with the proposed modification in requirement R1.4 reducing the amount of time allowed for making changes and updating the Cyber Security Incident Response Plan from 90 days to 30 days. The SDT agrees with the FERC Order in this situation which consistently requires a shortening of the update period. The 30-day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days

Several of the stakeholders recommend removal of the word “dated” from the measures for this standard. The SDT agrees and will remove the word “dated” at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.

Several of the stakeholders recommended wording changes to R.1 to clarify that the Responsible Entity shall develop and maintain a Cyber Security Incident response plan, and the plan shall be activated in response to a Cyber Security Incident, when such an incident occurs. The SDT will consider this change and many others as part of future phase revisions of the CIP standards.

A few stakeholders requested a clarification of the additional language detailing the requirements of the Cyber Security Incident response team, since the language implies Cyber Security specific training or a core set of knowledge requirements for the incident responders. The SDT confirmed that the response team members should be able to effectively perform the roles and responsibilities outlined in the Cyber Security Incident Response Plan.

One stakeholder asked if authorized exceptions result in non-compliance, citing situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The SDT confirmed that situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT made the following modification to CIP-008-2 based on stakeholder comments:

M1. The Responsible Entity shall make available its ~~dated~~ Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

Organization	Yes or No	Question 7 Comment
CenterPoint Energy	No	CenterPoint Energy strongly disagrees with the proposed modification in R1.4 reducing the amount of time allowed for making changes and updates to the Cyber Security Incident Response Plan from 90 days to 30 days. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any changes.
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Exelon	No	Recommendation to increase the timeframe in R1.4 to document changes to the cyber security incident response plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS questions the change in timing requirements for R1.4 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan not being updated within 90 days.
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Ontario Power Generation	No	Reducing the timeframe to update the Incident Response Plan from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.

Organization	Yes or No	Question 7 Comment
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Progress Energy	Yes	CIP008R1.4 – The reduction from 90 to 30 days is inadequate considering the coordination and approvals necessary. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
WECC Reliability Coordination	No	we feel that 90 days is a reasonable time frame.
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
Response: Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that “duly authorized exceptions will not result in non-compliance” within Section D-1.5 of the standard.		
Encari	No	1. We are confused about the necessity to call out a specific "Cyber Security Incident" response team.

Organization	Yes or No	Question 7 Comment
		Does this no longer require an entity to have a physical security incident response team? -- General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: 1. This standard relates to cyber security incident response only. An entity's physical security incident response may or may not be related. 2) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit. 3. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority. The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.		
Consolidated Edison Company of New York, Inc.	No	1) We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain and implement a Cyber Security Incident response

Organization	Yes or No	Question 7 Comment
		plan. The plan shall be activated in response to a Cyber Security Incident." 2) We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the Entity's Change Process" (see questions 5). 3) The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) Measure M1 is one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: 1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 4) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
ISO New England Inc	No	1) We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop. and maintain a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident, when such an incident occurs." 2) We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the Entity's Change Process" 3) The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.

Organization	Yes or No	Question 7 Comment
Response: 1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 4) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Northeast Power Coordinating Council	No	1) We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the entity's change process". 3) Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: 1)-2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 3) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Orange and Rockland Utilities Inc.	No	1) We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain, and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the Entity's Change Process" 3) The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident

Organization	Yes or No	Question 7 Comment
		response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: 1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 4) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Brazos Electric Power Cooperative, Inc.	No	In R1.3, replace "Process for reporting" with "Process for communicating reportable". In R1.4, replace "of any changes" with "of any procedural changes". In M2, replace "all documentation" with "all relevant documentation related to Cyber Security Incidents".
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Detroit Edison Company	No	1. The addition of "and implement the plan in response to Cyber Security Incidents." is awkward. This literally states that the plan will only be implemented upon a security incident, but the plan must be implemented in order to "characterize and classify" reportable Cyber Security Incidents. It might be clearer if written as "The Responsible Entity shall develop, implement and maintain a Cyber Security Incident Response Plan....and execute the plan in the event of a Cyber Security Incident." 2. Remove the "Process for ..." language in CIP-008-2 R1.4, R1.5, and R1.6 to be consistent with the language changes in CIP-006 R1.7 and R1.8. Suggested language is as follows: a. R1.4. Update of the Cyber Security Incident response plan within thirty calendar days of any changes. b. R1.5. Annual review of the Cyber Security Incident response plan. c. R1.6. Annual testing of the Cyber Security Incident response plan. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise,

Organization	Yes or No	Question 7 Comment
		to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.
Response: 1.-2. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Northern Indiana Public Service Company	No	In CIP-008-2 R1.2, I would like a clarification of the additional language detailing Cyber Security Incident response team requirements. This additional language implies Cyber Security specific training or a core set of knowledge requirements for the incident responders. What will be the measuring stick to determine if an incident responder is a Cyber Security Incident responder or a non-cyber security incident responder?
Response: Team members should be able to effectively perform the roles and responsibilities outlined in the Cyber Security Incident Response Plan. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Ontario IESO	No	The new sentence in R1.6 is not a requirement and does not add any value; in fact, it may create confusion - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence.
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
PPL Corporation	No	The sentence added to the end of R1.6 would be more appropriate in a FAQ, guideline, or interpretation rather than in the standard itself.
Response: The sentence added to the end of R1.6 was done in accordance with FERC Order 706. In Paragraph 687, the Commission clarified that with respect to full operational testing under CIP-008-1, “such testing need not require a responsible entity to remove any systems from service”.		

Organization	Yes or No	Question 7 Comment
Phase 1 of Project 2008-06 CSO706 includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Standards Review Committee of ISO/RTO Council	No	The new sentence in R1.6 is not a requirement and does not add any value; in fact, it may create confusion - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence.
Response: The sentence added to the end of R1.6 was done in accordance with FERC Order 706. In Paragraph 687, the Commission clarified that with respect to full operational testing under CIP-008-1, "such testing need not require a responsible entity to remove any systems from service". Phase 1 of Project 2008-06 CSO706 includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: "Responsible Entity" is defined within the Applicability section of each CIP standard. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Southern Company	Yes	CIP-008 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-008 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-008 Section D - Compliance: 1.4.2 - Should have a time limit to reduce the overall liability of

Organization	Yes or No	Question 7 Comment
		confidential information.
Response: 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405). 1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT. 1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.		
Deloitte & Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal incident management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: Reliability standards are limited to specifying what to do, not how to do it. Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.		
Alberta Electric System Operator	Yes	
Ameren	Yes	
American Transmission	Yes	

Organization	Yes or No	Question 7 Comment
Company		
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Bonneville Power Administration	Yes	
City of Tallahassee (TAL)	Yes	
Consumers Energy Company	Yes	
CoreTrace	Yes	
Duke Energy	Yes	
Dynegy	Yes	
FirstEnergy Corp	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
Manitoba Hydro	Yes	
MidAmerican Energy Company	Yes	

Organization	Yes or No	Question 7 Comment
Oncor Electric Delivery LLC	Yes	
PacifiCorp	Yes	
San Diego Gas and Electric Co.	Yes	
Southern California Edison Company	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
US Bureau of Reclamation	Yes	
Xcel Energy	Yes	

8. The CSO706 SDT revised the timeframe to thirty days for communicating updates of recovery plans to personnel responsible for activating or implementing the plan in **CIP-009-1** Requirement R3.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

While many stakeholders disagreed with the proposed modification in Requirement 3 of reducing the timeframe allowed for communicating updates of the recovery plans to personnel responsible for activating and implementing the plans from 90 days to 30 days, most stakeholders agreed with the change. The SDT agreed with most stakeholders and the FERC Order in this situation which consistently requires a shortening of the update period. The 30-day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days

Several of the stakeholders recommend removal of the word "dated" from the measures for this standard. The SDT agrees and will remove the word "dated" at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.

One stakeholder asked if authorized exceptions result in non-compliance, citing situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The SDT confirmed that situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception.

The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT made the following changes to CIP-009-2 based on stakeholder comments:

R1 Removed the following introductory phrase from the Requirements Section:

~~The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:~~

M1 through M5 Removed the word, "dated" from all measures.

Organization	Yes or No	Question 8 Comment
CenterPoint Energy	No	Regarding R3, CenterPoint Energy acknowledges that updates to a recovery plan and communication of those updates should be completed in a timely manner; however, CenterPoint Energy believes the SDT

Organization	Yes or No	Question 8 Comment
		went too far in reducing the timeframe for communicating updates from 90 days to 30 days. CenterPoint Energy believes that 30 days is too constraining. Furthermore, in FERC Order 706, paragraph 731, the Commission separated the time allowed for updating recovery plans (30 days) and the time allowed for communicating those updates (90 days), and was willing to consider timeframes other than 30 days. CenterPoint Energy proposes a 60 day window for updating a recovery plan and retaining the 90 day window for communicating the updates to responsible personnel. This would allow adequate time for the appropriate documentation changes to be made and is still timely for communicating to personnel.
Response: The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Exelon	No	Recommendation to increase the timeframe in R3 to require updates to be communicated within 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management activity.
Response: The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
ISO New England Inc	No	1 - We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2 - "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate.
Response: 1. The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives		

Organization	Yes or No	Question 8 Comment
included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 2. The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS questions the change in timing requirements for R3 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan(s) not being updated within 90 days.
Response: The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Northeast Power Coordinating Council	No	1) We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed." to "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of completion of the entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate.
Response: 1) The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days. 2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Northern Indiana Public Service Company	No	I do not agree with the reduction from 90 to 30 days. I would propose to provide uniformity and match the modified requirement under CIP-007-2 R9, which requires the modifications to be documented within 30 calendar days after completion versus the CIP-009-2 R3 language which requires the updates to be communicated within 30 calendar days after completion.

Organization	Yes or No	Question 8 Comment
Response: The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Ontario Power Generation	No	Reducing the timeframe to communicate updates to CCA recovery plans from within 90 to within 30 calendar days introduces a constraint that may not be achievable in a large organization.
Response: The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Orange and Rockland Utilities Inc.	No	1) We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
Response: 1) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 2) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Pepco Holdings, Inc - Affiliates	No	It may not be possible to communicate updates of recovery plans to all personnel responsible for activating or implementing the plan within 30 days (e.g. family leave). Suggest adding exceptions.

Organization	Yes or No	Question 8 Comment
Response: The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
WECC Relibaility Coordination	No	We feel 90 days is a reasonable time frame.
Response: The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: “Duly authorized exceptions will not result in non-compliance.”
Response: Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that “duly authorized exceptions will not result in non-compliance” within Section D-1.5 of the standard.		
Encari	No	General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 1) The wording of 1.1.1 is awkward and should be modified. 2) We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which

Organization	Yes or No	Question 8 Comment
		entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: 1) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit. 2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.		
Consolidated Edison Company of New York, Inc.	No	1) We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
Response: 1) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.		
Brazos Electric Power Cooperative, Inc.	No	In R3, replace "being completed" with "being effective".

Organization	Yes or No	Question 8 Comment
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
KEMA	Yes	In R1, it should be added that the Recovery Plans must be stored on site and a second copy off-site for responders in case the primary site is inaccessible.
Response: Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Progress Energy	Yes	CIP009-R3 – The reduction from 90 to 30 days is inadequate considering the coordination and approvals necessary. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.

Organization	Yes or No	Question 8 Comment
Response: "Responsible Entity" is defined within the Applicability section of each CIP standard. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.		
Alberta Electric System Operator	Yes	
Ameren	Yes	
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	

Organization	Yes or No	Question 8 Comment
Bonneville Power Administration	Yes	
City of Tallahassee (TAL)	Yes	
Consumers Energy Company	Yes	
CoreTrace	Yes	
Deloitte & Touche, LLP	Yes	
Detroit Edison Company	Yes	
Duke Energy	Yes	
Dynegy	Yes	
FirstEnergy Corp	Yes	
Kansas City Power & Light	Yes	
Luminant Power	Yes	
Manitoba Hydro	Yes	
MidAmerican Energy Company	Yes	
Old Dominion Electric Cooperative	Yes	
Oncor Electric Delivery LLC	Yes	

Organization	Yes or No	Question 8 Comment
Ontario IESO	Yes	
PacifiCorp	Yes	
PPL Corporation	Yes	
San Diego Gas and Electric Co.	Yes	
Southern California Edison Company	Yes	
Southern Company	Yes	
Standards Review Committee of ISO/RTO Council	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
US Bureau of Reclamation	Yes	
Xcel Energy	Yes	

9. The CSO706 SDT proposes the following for the **Effective Date**:

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

   Do you agree with the proposed Effective Date? If not, please explain and provide an alternative to the proposed effective date that would eliminate or minimize your disagreement.

Summary Consideration:

Many of the stakeholders requested clarification of the Effective Date of these standards. The SDT clarified that the NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

Some stakeholders expressed concern regarding the standards becoming effective at different dates in different jurisdictions. The SDT confirmed that where entities in different organizations are required to work cooperatively with one another using a common set of rules or procedures to support reliability, there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where no coordination exists between entities in different jurisdictions, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. The CIP standards are believed to fall into this second category.

Some stakeholders expressed concern about the applicability of the Effective Date to the CIP standards. The SDT confirmed that these Effectives Dates apply to the “Version 2” updates of these standards. The requirements in the proposed standards would replace similar requirements in existing standards. If an Entity were already expected to be compliant with a requirement in one of the “Version 1” CIP standards, then when the same requirement is replaced with its “Version 2” equivalent, the expectation is that the Entity has the evidence that was required under the Version 1 standard.

A few of the stakeholders requested clarification regarding the definition of the Violation Severity Levels (VSLs) for these CIP standards. The SDT clarified that the VSLs will be developed for these Version 2 Cyber Security Standards following the complete development of the VSLs for the Version 1 standards.

Several of the stakeholders requested clarification on the extent of the data retention requirements for audits. The SDT clarified that the “last audit record” would include the information from the last formal audit. If an entity was found non-compliant and a mitigation plan with milestones was developed, then the subsequent audit records would include the mitigation plan and associated documentation.

A few stakeholders requested clarification regarding the New Critical Cyber Asset Implementation Plan which would be applicable to newly identified Critical Assets and supersedes the Version 2 implementation schedule. The SDT clarified that the New Critical Cyber Asset Implementation Plan incorporates Table 4 of the Version 1 Implementation Plan and supersedes the Version 1 Implementation Plan. The New Critical Cyber Asset Implementation Plan states that "the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the [compliant] milestone listed in this Implementation Plan."

The SDT does not anticipate any additional comment periods for the Phase 1 revisions to the CIP standards. The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

The SDT did not make any changes to the proposed effective date based on stakeholder comments.

Organization	Yes or No	Question 9 Comment
Consolidated Edison Company of New York, Inc.	No	1. Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2. Request confirmation that these Effectives Dates apply to these updates (Version 2) 3. We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4. We request clarification on Compliance 1.1.1. Wording is confusing. 5. While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6. When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7. There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009

Organization	Yes or No	Question 9 Comment
Response: 1. The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language. For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations. 2. The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved. 3. The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards. 4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. 5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures. Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws. 6. The Violation Severity Levels (VSLs) for these Version 2 Cyber Security standards will be developed following the complete development of the VSLs for the Version 1 standards. 7. The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.		
Detroit Edison Company	No	Does this mean that the current quarter must end, and then you start counting to the first day of the following 3 quarters, or do you include the current quarter in counting? Why not simplify things and use a number of days, such as: "120 calendar days after applicable regulatory approvals have been received . . . . . ."

Organization	Yes or No	Question 9 Comment
Response: The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.		
Encari	No	This effective date is still open-ended as the process is not complete. Once additional comment periods have completed and the revisions have been refined we will provide comment as to the acceptability of this timeframe and the continued assurances of the reliability of the Bulk Electric System. We recommend that the standards become agreed upon and complete and then an effective implementation date be identified. This will provide proper assurances from asset owners that they can indeed meet the timeframe identified while continuing to assure the reliability of the BES. We also are confused regarding the term "calendar quarter" versus a concept of "fiscal quarter". Please provide a clarification.
Response: The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.		
ISO New England Inc	No	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing.

Organization	Yes or No	Question 9 Comment
		5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009.

Response:

1. The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.
2. For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.
3. The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.
4. The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.
5. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.

   The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.

   Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.
6. The Violation Severity Levels (VSLs) for these Version 2 Cyber Security Standards will be developed following the complete development of the VSLs for the Version 1 standards.
7. The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation

Organization	Yes or No	Question 9 Comment
plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.		
MidAmerican Energy Company	No	Comment: This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule. MidAmerican Energy Company has been working toward compliance with the standards under the premise that the generation owner has till December 31, 2009, to become compliant with version 1 standards. For significant changes proposed in version 2, the generation owner will need time to address and comply. For applicable regulatory approvals received between January 1 and March 31, revised standards will be effective the following January 1.MEC proposes the following language: Effective Date: The first day of the calendar quarter after at least nine months following the applicable regulatory approvals have been received, as illustrated in the following table. Applicable regulatory approval received - Effective the following Jan. 1- Mar. 31 Jan. 1Apr. 1- June 30 Apr.1July 1- Sept. 30 July 1Oct. 1- Dec. 31 Oct. 1
Response: The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions. The drafting team believes the six to nine month implementation plan is reasonable.		
Northeast Power Coordinating Council	No	1) Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)". In addition, Canadian members of NPCC have concerns regarding the standards becoming effective at different dates in different jurisdictions. Coordination is required among government authorities to ensure that standards become effective at the same time in all jurisdictions. 2) Request confirmation that these Effective Dates apply to these updates (Version 2). 3) We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4) We request clarification on Compliance 1.1.1. Wording is confusing. 5) While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary, the new terms are not (Regional Entity and Compliance Enforcement Authority).

Organization	Yes or No	Question 9 Comment
		6) When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7) Clarification required for "the last audit records" and "subsequent audit records" in Data Retention 1.4.2. This comment applies to CIP-002 - CIP-009.

Response:

1) The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

   For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2) The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.

3) The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.

4) 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.

5) The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.

   Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.

6) The Violation Severity Levels (VSLs) for these Version 2 Cyber Security Standards will be developed following the complete development of the VSLs for the Version 1 standards.

7) The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation

Organization	Yes or No	Question 9 Comment
plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.		
Northern Indiana Public Service Company	No	I have difficulty responding with acceptance or denial of an implementation schedule when I am not fully aware of what the final draft is going to consist of. Secondly, as this language stands I would like to see a proposed time line based on an example NERC BOT adoption date. I am unclear on weather the Version 2 standards would be implemented in parallel with the existing version 1 implementation schedule, in series, or only begin implementation after FERC approval as this draft is occurring due to FERC directed changes. I am also slightly confused on the audit process and which version of various CIP requirements would be applicable as the responsible entities move into an AC status, while the Version 2 standards could be BOT approved but not FERC approved.
Response: The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year. The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions. The New Critical Cyber Asset Implementation Plan incorporates Table 4 of the Version 1 Implementation Plan and supersedes the Version 1 Implementation Plan. The New Critical Cyber Asset Implementation Plan states that “the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be ‘Auditably Compliant’) one year following the [compliant] milestone listed in this Implementation Plan.”		
Orange and Rockland Utilities Inc.	No	1. Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)"

Organization	Yes or No	Question 9 Comment
		2. Request confirmation that these Effectives Dates apply to these updates (Version 2) 3. We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4. We request clarification on Compliance 1.1.1. Wording is confusing. 5. While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6. When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7. There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009

Response:

1. The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.

   For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.

3. The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.

4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.

5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in

Organization	Yes or No	Question 9 Comment
the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures. Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws. 6. The Violation Severity Levels (VSLs) for these Version 2 Cyber Security Standards will be developed following the complete development of the VSLs for the Version 1 standards. 7. The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.		
PacifiCorp	No	This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule found in Table 3. PacifiCorp has been working toward compliance with the standards under the premise that the generation owner has until December 31, 2009, to become compliant with Version 1 standards. For significant changes proposed in Version 2, the generation owner will need time to address and comply.
Response: The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.		
Pepco Holdings, Inc - Affiliates	Yes	Please consider adding in parenthesis "approximately 270 days" after "the third calendar quarter" for clarification. "The first day of the third calendar quarter (approximately 270 days) after applicable approvals?"
Response: The NERC Compliance program has requested the implementation date start on a calendar quarter January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.		
Progress Energy	No	PE would like clarification on the effective date Section A.5 of each standard. Given the nature of some of the requirements to possibly include significant capital investment, we want to ensure there is adequate time given for budget cycle and outage planning. Also, the guidance for identification of CAs is still incomplete which could impact implementation timeframes. PE recommends allowing 12 months after the BOT approval for the effective date.

Organization	Yes or No	Question 9 Comment
Response: The NERC Compliance program has requested the implementation date start on a calendar quarter (January, April, July, October). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year. The drafting team believes the six to nine month implementation plan is reasonable. The New Critical Cyber Asset Implementation Plan is applicable to newly identified CAs and supersedes the Version 2 implementation schedule.		
Southern California Edison Company	No	Wording is ambiguous. SCE suggests "six (6) months from date of approval."
Response: The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.		
American Electric Power	Yes	To add further clarity, AEP suggests that the following text be added to the effective date statement above." . . . after applicable FERC approvals have been received and such approval is posted in the public registry (or the . . . "
Response: The SDT does not feel that a change to the standard language is necessary. The US Federal Rulemaking Process requires that the effective date of the approval rule is contained in the text of the Final Rule that is published in the Federal Register.		
Ameren	Yes	

Organization	Yes or No	Question 9 Comment
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Bonneville Power Administration	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
City of Tallahassee (TAL)	Yes	It is confusing though.
Response: Thank you for your comment.		
Consumers Energy Company	Yes	
CoreTrace	Yes	
Deloitte & Touche, LLP	Yes	
Duke Energy	Yes	
Dynegy	Yes	

Organization	Yes or No	Question 9 Comment
Exelon	Yes	
FirstEnergy Corp	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
Manitoba Hydro	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Old Dominion Electric Cooperative	Yes	
Oncor Electric Delivery LLC	Yes	
Ontario IESO	Yes	
PPL Corporation	Yes	
San Diego Gas and Electric Co.	Yes	
Southern Company	Yes	
Standards Review Committee of ISO/RTO Council	Yes	
Tampa Electric	Yes	

Organization	Yes or No	Question 9 Comment
Company		
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
US Bureau of Reclamation	Yes	
WECC Reliability Coordination	Yes	
Xcel Energy	Yes	

10. The CSO706 SDT is proposing a separate **CIP implementation plan** to address newly identified Critical Cyber Assets. In this plan, three specific classes of categories for newly identified Critical Cyber Assets are described. The plan provides an implementation schedule with "Compliant" milestones for each requirement in each category. All timelines are specified as an offset from the date when the Critical Cyber Asset has been newly identified.

Do you agree with the approach proposed by the SDT for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement.

Summary Consideration:

A few of the stakeholders expressed concern about a Responsible Entity's mis-application of their risk assessment methodology and related omission to declare a Cyber Asset as critical. The SDT clarified that the Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.

One stakeholder requested clarification concerning the applicability of the Implementation Plan in the event of a merger or acquisition of a two companies. The SDT clarified that if the merger or acquisition resulted in a single registered entity, when both entities have existing programs, the Implementation Plan allows one year for the programs to be harmonized. When only one of the entities has an existing program, that program is expected to continue after the merger. In cases where the acquisition of assets results in a change in registered entity, if the acquiring company has a program and the acquired asset is already identified as critical, there is one year to harmonize the programs. If the acquiring company does not have a program and the acquired asset is already identified as critical, continuation of the program at the acquired asset is expected to be provided for in the acquisition process, assuming the asset continues to be critical.

A few stakeholders requested a change in the applicable timeframe after a new Critical Cyber Asset (CCA) is identified. The SDT agreed with the comment and will modify the applicable timeframe to 18 months after the new CCA is identified for Category 2 for CIP-004 Requirements R2, R3, and R4.

The drafting team does not anticipate additional comment periods for the Phase I revisions to the CIP standards. The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

Organization	Yes or No	Question 10 Comment
Dynegy	No	Under the Category 2 heading, the proposed method for handling the case of a business merger or acquisition when any of the Responsible Entities involved had previously identified Critical Cyber Assets is inequitable and inconsistent with the proposed handling of the case when all Registered Entities have

Organization	Yes or No	Question 10 Comment
		identified Critical Cyber Assets. Under the Category 2 heading, in the case of a business merger or acquisition when any of the Responsible Entities involved had previously identified Critical Cyber Assets, it really only matters if the acquiring or controlling Responsible Entity had previously identified Critical Cyber Assets. If the acquiring or controlling entity had not previously identified any Critical Cyber Assets it will have no CIP Compliance Program and it should be required to meet the same Category 1 (instead of Category 2) milestones established for the case where neither Registered Entity involved in merger had previously identified any critical Cyber Assets. In addition, in the case when all Registered Entities involved in a merger have identified Critical Cyber Assets the merged Responsible Entity is required to meet Category 2 milestones after one calendar year from the merger date. This provision in effect grants the Merged Responsibility Entity in this case the approximate equivalent of having to meet Category 1 milestones. This approach further justifies the revised approach suggested above for the former case.
Response: In the event of a merger or acquisition of a company resulting in a single registered entity, when both entities have existing programs, the Implementation Plan allows one year for the programs to be harmonized. When only one of the entities has an existing program, that program is expected to continue after the merger. In the case of acquisitions of assets resulting in a change in registered entity, if the acquiring company has a program and the acquired asset is already identified as critical, there is one year to harmonize the programs. If the acquiring company does not have a program and the acquired asset is already identified as critical, continuation of the program at the acquired asset is expected to be provided for in the acquisition process, assuming the asset continues to be critical.		
Ontario Power Generation	No	We note that the implementation plan for newly identified Critical Cyber Assets specifies that it applies to "CIP-002-1 through CIP-009-1 and their successor standards". We further notice that in Milestone Category 2 an number of requirements have a six (6) month timeframe specified for compliance. In effect, the identification of a new CCA at an Entity today would be required to be fully compliant with respect to that new newly identified CCA before December 31, 2009 - the Compliant deadline for all other CCAs.
Response: The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.		

Organization	Yes or No	Question 10 Comment
Oncor Electric Delivery LLC	No	The timeframes in Table 2 are reasonable. However, CIP-002-1 currently specifies that an asset is not designated as a Critical Asset until the annual application of the Risk-Based Methodology. A cyber asset is not a Critical Cyber Asset unless it is essential to the operation of the Critical Asset. Category 3 "Compliant upon Commissioning" is not a current requirement of CIP-002-1 and represents a significant change to the current standard. This seems to imply that the Risk-Based Methodology must be applied continuously, not just annually. "Compliant upon Commissioning" should only apply to replacing existing Critical Cyber Assets. New Critical Cyber Assets identified by CIP-002-1 Requirement R3 should utilize the timeframes in Category 2
Response: CIP-002-2, Requirements R2 (Critical Asset identification) and R3 (Critical Cyber Asset identification) state "the Responsible Entity shall review this list at least annually, and update it as necessary." These requirements expect the entity to assess the new asset or Cyber Asset as part of the planning process.		
FirstEnergy Corp	No	While we do agree with the overall objective the team is trying to achieve, we do not agree as presently written and offer the following comments: a) The description of Category 1 seems to imply that a Responsible Entity who has a CIP CA and CCA methodology, but did not identify any CCA assets may be given additional time to comply with the CIP standards when they have identified any CCAs on subsequent annual reviews. However, what is not clear is what triggered the new CCA being identified? The Category 1 description should be clear that it does not apply simply based on "error and ommission" if the Responsible Entity's methodologies for CA and CCA identification have not changed and the Responsible Entity simply overlooked an asset that should have been previously identified and protected. If these newly identified assets were in service during their initial CIP asset determination, then the entity was not compliant with their initial asset identification and it should be expected that the entity would file a Self Report and Mitigation Plan to obtain compliance. b) FE believes our above comment on Category 1 also applies to the Category 2 description as it indicates in the second paragraph that it refers to newly identified CCA assets but they are not associated with an addition or modification through construction, upgrade or replacement. Again, if the methodologies have not changed, if there was no merger or acquisition, then what triggered the newly identified existing asset? It should be clear that "error and ommission" do not apply. c) We agree with the provisions described for newly acquired assets through mergers and acquisitions when companies may have had differing methodologies. d) We agree with item 3 regarding "Compliant upon Commissioning" for newly planned upgrades that result in new CA and CCA items. e) In general we found the information to be overly wordy and confusing to understand. We suggest the

Organization	Yes or No	Question 10 Comment
		team attempt to greatly consolidate the information. f) Tables 2 should be adjusted such that it can be read and viewed stand alone to the extent possible from the remaining supporting text. For example, Table 2 has no indication that the numbers refer to "months".
Response: a) The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation. b) The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation. c) Thank you for your comment. d) Thank you for your comment. e) The posted version is simplified from early drafts and must address the complexity of the problem. f) The tables will be updated to reflect the time period as being in months.		
Consolidated Edison Company of New York, Inc.	No	1) On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2) We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some reference Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3) We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4) We request clarification on historical records for Category 3 (Compliant upon Commissioning) Critical Cyber Assets 5) Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6) Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified

Organization	Yes or No	Question 10 Comment
		through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7) We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8) We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9) There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
Response: 1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that entity 12 months to comply. 2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All applicable references to Version 1 of the standards within the document will be similarly modified. 3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan. 4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date. New assets will not have a full year of audit data available when they are identified as critical. 5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief. 6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 8) The SDT agrees with the recommendation. 9) The SDT agrees with the comment and will change the title of the document accordingly.		
ISO New England Inc	No	1) On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these

Organization	Yes or No	Question 10 Comment
		Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2) We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some references Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3) We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4) We request clarification on historical records for Category 3 (Compliant upon Commissioning) Critical Cyber Assets 5) Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6) Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7) We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8) We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9) There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that entity 12 months to comply.

2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read “Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards.” All applicable references to Version 1 of the standards within the document will be similarly modified.

3) “Category 3” does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.

4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the

Organization	Yes or No	Question 10 Comment
		Compliance Date. New assets will not have a full year of audit data available when they are identified as critical. 5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief. 6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 8) The SDT agrees with the recommendation. 9) The SDT agrees with the comment and will change the title of the document accordingly.
Northeast Power Coordinating Council	No	1) On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that the CIP-003 R2 Requirement (wherever it is) should be 12 months. 2) We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some refer to Version 2 (Table 2), and the Requirements do not match CIP-006-2. 3) We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon Commissioning." 4) We request clarification on historical records for Category 3 (Compliant upon Commissioning) Critical Cyber Assets. 5) Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence. 6) Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7) We recommend an additional scenario where a failed Cyber Asset in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial communications and the new Asset uses IP communications. We suggest this is Category 2.

Organization	Yes or No	Question 10 Comment
		8) We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9) There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
Response: 1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that entity 12 months to comply. 2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All applicable references to Version 1 of the standards within the document will be similarly modified. 3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan. 4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date. New assets will not have a full year of audit data available when they are identified as critical. 5) The SDT agrees that the CCAs should remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief. The SDT is concerned that if the sentence is removed, entities may remove the assets from service in order to not be found in non-compliance of the standard, resulting in a "detrimental effect on the grid." Similarly, changing the sentence to require that the assets must remain in service would not allow a brief maintenance outage to allow entities to implement changes associated with bringing the assets into compliance. 6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 8) The SDT agrees with the recommendation. 9) The SDT agrees with the comment and will change the title of the document accordingly.		
Orange and Rockland Utilities Inc.	No	1) On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2) We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan is applies to Version 2 because some references

Organization	Yes or No	Question 10 Comment
		Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3) We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4) We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5) Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6) Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7) We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8) We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9) There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that entity 12 months to comply.

2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read “Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards.” All applicable references to Version 1 of the standards within the document will be similarly modified.

3) “Category 3” does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.

4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date. New assets will not have a full year of audit data available when they are identified as critical.

5) The SDT agrees that the CCAs must remain in service to avoid a “detrimental effect on the grid.” The inclusion of this sentence reinforces that belief.

Organization	Yes or No	Question 10 Comment
6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. 8) The SDT agrees with the recommendation. 9) The SDT agrees with the comment and will change the title of the document accordingly.		
Encari	No	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period.
Response: The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards.		
Manitoba Hydro	No	The new implementation plan needs to clearly state that the categorization is only applied to newly identified Critical Cyber Assets, and not to all Critical Cyber Assets. The new implementation plan should also state that the categorization of a Critical Cyber Asset expires and is no longer required when that Critical Cyber Asset becomes compliant. Table 2 needs to indicate that the milestones listed are in months. The title for Table 3 needs to be revised to indicate that the table is to be used for Registered Entities which have identified their first Critical Cyber Asset (Category 1), and for newly Registered Entities.
Response: The New Critical Cyber Asset Implementation Plan repeatedly refers to "newly identified" Critical Cyber Assets. "Compliant Upon Commissioning" also includes Cyber Assets replacing existing Critical Cyber Assets. The categorization is only used to determine the applicable compliance schedule and has no meaning once the Critical Cyber Asset is compliant. The tables will be updated to reflect the time period as being in months. Table 2 is applicable to all Registered Entities that have now identified their first Critical Cyber Asset (Category 1) after registration. Table 3 is only applicable to newly Registered Entities whether or not they have identified a Critical Asset.		
Northern Indiana Public Service Company	No	Moving through the existing phases, I do not believe the steps provide for a situation in which a utility wishes to improve or strengthen the risk-based methodology. If a utility has an existing CCA and strengthens the methodology process which in turn produces a new CA and in turn new CCA's, the

Organization	Yes or No	Question 10 Comment
		utility would find itself in immediate non-compliance. Based on this situation and using the flow chart contained within the proposed implementation schedule document, the responsible entity would already have an existing CCA, the Cyber assets of the new resulting CA would already be in service, and it would be a planned change as the utility chose to strengthen the existing methodology. The flow chart result would be compliant upon commissioning, and the cyber asset is already in service, therefore the real world result is immediate non-compliance. I believe this is counter productive as NERC and FERC would encourage an entity to strengthen the risk-based methodology. The current proposed implementation schedule would encourage a utility to not strengthen the risk-based methodology over time in order to remain in compliance. I believe additional provisions need to be made.
Response: The described scenario is defined in Table 1 “Example Scenarios”. The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail.		
Exelon	Yes	The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
Response: The SDT agrees with the comment and will modify the timeframe to 18 months after the new CCA is identified for Category 2 for CIP-004 Requirements R2, R3, and R4.		
Deloitte & Touche, LLP	Yes	Will the drafting team include situations that occur through merger and acquisition (M&A)?
Response: Merger and Acquisition is addressed in the New Cyber Asset Implementation Plan.		
Ameren	Yes	Would like to see a clarification on what is intended by phrase "planned change".
Response: A “planned change” is any anticipated and planned for change to an asset or Cyber Asset.		
Electric Market Policy	Yes	1) "Responsible Entity" is not defined in the implementation plan. 2) On page 1 under Implementation Schedule, Item #3 should read: "A new or existing "Cyber" Asset becomes?"

Organization	Yes or No	Question 10 Comment
		3) On page 2, the first sentence should reference "other" Cyber Assets rather than "non-critical" Cyber Assets to be consistent with the red-line change to CIP-007-2 Purpose. 4) On page 4, bullet "b" perimeter needs to be capitalized.
Response: 1) Responsible Entity is defined in the language of each standard. 2) The SDT agrees with the recommendation. 3) The SDT agrees with the recommendation. 4) The SDT agrees with the recommendation.		
City of Tallahassee (TAL)	Yes	Although it can be confusing also.
Response: The posted version is simplified from early drafts and must address the complexity of the problem.		
American Electric Power	Yes	
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Bonneville Power Administration	Yes	
Consumers Energy Company	Yes	

Organization	Yes or No	Question 10 Comment
Detroit Edison Company	Yes	
Duke Energy	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
MidAmerican Energy Company	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Old Dominion Electric Cooperative	Yes	
Ontario IESO	Yes	We believe the proposed implementation plan is reasonable and appropriate.
Response: Thank you for your comment.		
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	We specifically appreciate and support the CSO706 SDT efforts in closing the current gap in the CIP standards for compliance of newly identified Critical Cyber Assets by creating three categories with a related implementation schedule.
Response: Thank you for your comment.		
PPL Corporation	Yes	PPL agrees with different categories of newly identified Critical Cyber Assets and the different

Organization	Yes or No	Question 10 Comment
		implementation schedule for these classes of categories.
Response: Thank you for your comment.		
Progress Energy	Yes	
San Diego Gas and Electric Co.	Yes	
Southern California Edison Company	Yes	
Southern Company	Yes	
Standards Review Committee of ISO/RTO Council	Yes	We believe the proposed implementation plan is reasonable and appropriate.
Response: Thank you for your comment.		
Tampa Electric Company	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
US Bureau of Reclamation	Yes	

Organization	Yes or No	Question 10 Comment
WECC Reliability Coordination	Yes	
Xcel Energy	Yes	

11. Do you agree with the **compliance milestones** included in the proposed implementation plan for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement..

Summary Consideration:

Many of the stakeholders requested that the time period requirements expressed in the Implementation Tables be consistently provided in months. The SDT agreed with this request and has updated the Implementation Tables accordingly.

A few stakeholders requested clarification of the Implementation Plan timeframe for Category 1 and Category 2. The SDT clarified that the Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. An Entity that cannot comply within the implementation plan will be expected to submit a self-report of non-compliance with a mitigation plan to achieve compliance.

One stakeholder requested clarification regarding the Implementation Plan of New Critical Cyber Assets. The SDT clarified that the Compliant and Auditably Compliant Milestones identified in the New Critical Cyber Asset Implementation Plan are meant to be separate and distinct. The New Critical Cyber Asset Implementation Plan states that "the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the [compliant] milestone listed in this Implementation Plan."

The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

Organization	Yes or No	Question 11 Comment
Manitoba Hydro	No	CIP-003-2 R3, R4, and R5: The milestones should be changed to 6 months. Although the information protection, access control and change control and configuration management programs exist, the requirements also include implementation, which will require some time to meet compliance. CIP-008-2 R2: The milestone should be changed to 6 months, the same as R1. The documentation required in R2 is dependent upon the elements in the Cyber Security Incident Response Plan developed in R1. CIP-009-2 R2 and R3: The milestones should be changed to 6 months, the same as R1. The exercises and change control in R2 and R3 are dependent upon the elements in the Recovery Plan developed in

Organization	Yes or No	Question 11 Comment
		R1.
Response: The SDT interprets the comments to refer to Milestone Category 2. CIP-003, Requirement R3 has no implementation requirements, and thus the current timeframe is reasonable. The SDT will modify the Category 2 compliance timeframe for CIP-003-2 Requirements R4, R5, and R6 to be 6 months. The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended. The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.		
Northern Indiana Public Service Company	No	I do not believe CIP-003-2 R3-R6 should be assumed to exist under Category 2 assets. An entity may need to identify exceptions, information, provide access control to that information and implement change control procedures on the newly identified asset. I also do not believe that it should be assumed that an entity can obtain the necessary financial capital to implement systems for compliance in any immediate fashion.
Response: The SDT will modify the Category 2 compliance timeframe for CIP-003-2 Requirements R4, R5, and R6 to be 6 months. An entity that cannot comply within the implementation plan will be expected to submit a self-report of non-compliance with a mitigation plan that provides sufficient time to obtain funding.		
Ontario Power Generation	No	We interpret that the plan seems to collapse together the Compliant and Auditably Compliant milestones. We note that it is not possible to identify a new CCA, bring it into a state or Compliant (as defined in the currently applicable standard) and have one year of data and records as required to be Auditably Compliant. We believe clarification is required in this area.
Response: The Compliant and Auditably Compliant Milestones identified in the New Critical Cyber Asset Implementation Plan are meant to be separate and distinct. The New Critical Cyber Asset Implementation Plan states that "the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the [compliant] milestone listed in this Implementation Plan."		
PPL Corporation	No	PPL has concerns with the existing implementation schedule. Table 2 identifies some standard requirements as existing for Category 2 milestones. Having an Information Protection program does not

Organization	Yes or No	Question 11 Comment
		mean that all information associated with a newly identified Critical Cyber Asset is immediately protected. For example, if an RE identifies an asset as critical with critical cyber assets, not all drawings and documentation will exist immediately marked as such. Even existing programs need to be applied to newly identified assets requiring an implementation schedule. The second concern is dependent on the outcome of the FERC Order for Clarification of CIP standards applicability to nuclear generating facilities. If the FERC Order results in nuclear facilities being included in the CIP applicability, this implementation plan should be noted to not include nuclear facilities affected by the pending FERC Order. The FERC Clarification Order needs to address the schedule for including nuclear facilities in the CIP applicability.
Response: The SDT agrees with the example cited and will modify the Category 2 compliance time frame for CIP-003-2 Requirements R4, R5, and R6 to be 6 months. The issue of nuclear facilities is out of scope for this drafting team.		
Progress Energy	No	The implementation plan for new CAs and CCAs allows 6-12-24 months for compliance, as noted by standard for Category 1-2 programs. For Category 2 programs (CIP program in place), for those requirements needing capitol funding anything less than 18 months would be difficult due to funding requests/process for capital. PE recommends those requirements potentially requiring significant capitol investment allowing a minimum of 18 months for compliance.
Response: An entity that cannot comply within the implementation plan will be expected to submit a self-report of non-compliance with a mitigation plan that provides sufficient time to obtain funding.		

Organization	Yes or No	Question 11 Comment
US Bureau of Reclamation	No	The agreement would be based on the response to the CIP-004 background check requirement timeframe. The milestones would require adjustment for more exhaustive background checks.
Response: Personnel can be granted unescorted access as long as a personnel risk assessment has been conducted according to the requirements in CIP-004 R3. A more exhaustive background check is not required; therefore an adjustment to the implementation plan is not necessary.		
Encari	No	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period. For instance, the current document details "existing" within CIP-003-2; however - newly identified CCAs may not immediately be able to compliant at zero day with CIP-003-2 requirements. For example R4 requires the information associated with the CCA to be protected. This information may still reside in a non-protected format prior to becoming a CCA - however the implementation timeframe is "existing".
Response: The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The SDT agrees with the example cited and will modify the Category 2 compliance time frame for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.		
Consolidated Edison Company of New York, Inc.	No	1) - We recommend that Table 2 clarifies the units as months, per page 1 2) - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3) - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: 1) The tables will be updated to reflect the time period as being in months. 2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended. 3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.		

Organization	Yes or No	Question 11 Comment
Detroit Edison Company	No	Table 2 does not address CIP-006-2 R7 and R8. They should both be 24 for category 1 and 12 for category 2. Table 2 CIP-008-2 R2 category 2 should be changed from 0 to 6 which matches the timetable associated with R1. The 0 implies that a Responsible Entity needs to retain documents relating to requirement, R1.1, which that entity is not yet required to be compliant. Table 2 CIP-009-2 R2 and R3 category 2 should be changed from 0 to 12. Similarly to the comment around CIP-008-2 R2, a Responsible Entity cannot be compliant with exercising a plan that is not required to exist. Changing the timetable to 12 ensures the recovery plan is initially executed in the annual time frame required by R2.
Response: Table 2 does not reflect the addition of two new requirements in CIP-006-2. The SDT will update the tables appropriately. The formal title and references to the CIP standards will be modified to refer to the Version 2 standards and their successors. The SDT will update Table 2 CIP-008-2 R2 category 2 to 6 months as recommended. The SDT will update Table 2 CIP-009-2 R2 and R3 category 2 to 12 months as recommended.		
Exelon	No	The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
Response: The SDT agrees with the comment and will modify the timeframe to 18 months after the new CCA is identified for Category 2 for CIP-004 Requirements R2, R3 and R4.		

Organization	Yes or No	Question 11 Comment
ISO New England Inc	No	1 - We recommend that Table 2 clarifies the units as months, per page 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: 1) The tables will be updated to reflect the time period as being in months. 2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended. 3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.		
Northeast Power Coordinating Council	No	1 - We recommend that Table 2 clarify the units as months, per page 1. 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 – Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: 1) The tables will be updated to reflect the time period as being in months. 2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended. 3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.		
Orange and Rockland Utilities Inc.	No	1 - We recommend that Table 2 clarifies the units as months, per page 1 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.

Organization	Yes or No	Question 11 Comment
Response: 1) The tables will be updated to reflect the time period as being in months. 2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended. 3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.		
FirstEnergy Corp	Yes	We agree with the Implementation Plan times described for Category 1 and Category 2, however, we believe clarification is need as to when these provisions apply. See our comments in Question 10.
Response: The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.		
Electric Market Policy	Yes	On page 6, Table 2 Milestone Categories should indicate "months."
Response: The tables will be updated to reflect the time period as being in months.		
Ameren	Yes	
American Electric Power	Yes	
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	

Organization	Yes or No	Question 11 Comment
Bonneville Power Administration	Yes	
City of Tallahassee (TAL)	Yes	
Consumers Energy Company	Yes	
Deloitte & Touche, LLP	Yes	
Duke Energy	Yes	
Dynegy	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Luminant Power	Yes	
MidAmerican Energy Company	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Old Dominion Electric Cooperative	Yes	
Oncor Electric Delivery LLC	Yes	
Ontario IESO	Yes	We believe the proposed implementation plan is reasonable and appropriate.

Organization	Yes or No	Question 11 Comment
Response: Thank you for your comment.		
PacifiCorp	Yes	
San Diego Gas and Electric Co.	Yes	
Southern California Edison Company	Yes	
Southern Company	Yes	
Standards Review Committee of ISO/RTO Council	Yes	We believe the proposed implementation plan is reasonable and appropriate.
Response: Thank you for your comment.		
Tampa Electric Company	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
WECC Reliability Coordination	Yes	

Organization	Yes or No	Question 11 Comment
Xcel Energy	Yes	

12. The CSO706 SDT seeks input on whether to include the information contained in this **stand-alone implementation plan within the body of each standard.** This would likely entail a new requirement in CIP-002 to classify newly identified Critical Cyber Assets, and changes to the remaining standards to insert the milestone timeframes.

    Do you agree with including the information about newly identified Critical Cyber Assets and newly registered entity information within the body of the standards which would eliminate the stand-alone documents? If not, please explain.

Summary Consideration:

A number of the stakeholders agreed that the New Critical Cyber Asset Implementation Plan should be maintained as a separate document from the standards. The SDT agrees and will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.

One stakeholder questioned why any newly installed asset would be considered anything but critical. The SDT clarified that there may be multiple reasons for building a Bulk Electric System (BES) asset, including reliability or economic. It is left up to the Responsible Entity to determine if the newly built asset is a Critical Asset based on its impact to the reliability of the BES.

The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

Organization	Yes or No	Question 12 Comment
Bonneville Power Administration	No	Including the implementation plan information in the individual CIP standards would greatly increase the size and complexity of each standard. All NERC Reliability Standards, including CIP, must be interpreted using various stand-alone documents (e.g., NERC Glossary of Terms Used in the Reliability Standards, NERC Reliability Functional Model, Compliance Monitoring and Enforcement Program, etc.). It's not a problem having the Implementation Plan available as a separate link or as a companion document to the CIP Reliability Standards.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		

Organization	Yes or No	Question 12 Comment
CoreTrace	No	To include the distinct procedures for newly identified Critical Cyber Assets would introduce a level of complexity and confusion into the current standard. As they stand today the CIP requirements are easy to understand and useful. A reference to the standalone implementation plan in the CIP body would be useful and sufficient and ensure that the information in the implementation plan was not overlooked.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Encari	No	We agree that the requirement to identify new CCA should be included; however, we believe that a continued need to guide Responsible Entities in the selection of CAs and CCAs is still necessary as separate documents.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision. Guidelines for the identification of Critical Assets and Critical Cyber Assets are currently being developed.		
FirstEnergy Corp	No	The stand alone document is sufficient and could be easily added as a reference document to each standard.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
KEMA	No	Any change to the Standards is a long a laborious effort, so a change in implementation plan will have to go through the process. A separate document with the plan facilitites changes to the plan and not the Standard.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		

Organization	Yes or No	Question 12 Comment
Ontario IESO	No	We believe that an implementation plan managed as a separate document is a more logical choice. Information is less likely to be repetitive and other standards can reference it as necessary. However, where an issue pertains to a single standard, it would be appropriate to include the pertinent implementation information within that standard.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Progress Energy	No	PE recommends referring to the implementation plan but not including it in the standard.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
San Diego Gas and Electric Co.	No	For clarity, SDG&E prefers the stand-alone Implementation Plan documents as presented rather than integrating the information for newly identified CCAs and newly registered entities into the existing CIP standards. This will help eliminate confusion and keep the existing Standard requirements and new CCAs/Registered Entity information separate.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Standards Review Committee of ISO/RTO Council	No	We believe an implementation plan managed as a separate document is a more logical choice. Information is less likely to be repetitive and other standards can reference it as necessary. However, where an issue pertains to a single standard, it would be appropriate to include the pertinent implementation information within that standard.

Organization	Yes or No	Question 12 Comment
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
US Bureau of Reclamation	No	Inserting the information and time lines for newly identified Critical Cyber Assets and newly registered entity information into the body of the standards will cause unnecessary confusion regarding the implementation of the standards. By retaining the current stand-alone implementation plan it provides a ready reference and single point of information for all new Critical Cyber Assets and newly registered entities.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Austin Energy	No	I have a question as to why any newly installed asset would be anything but critical. Certainly existing assets can degrade to a point where they no longer fulfill a critical role, but why would a new asset be installed if there was not a need?
Response: There may be multiple reasons for building a Bulk Electric System (BES) asset, including reliability or economic. Other reasons might include transmission to connect a new merchant generator (which may have economic benefit to the GO, but not necessarily the TO), or BES assets supporting increased retail or wholesale load. Alternatively, a parallel implementation to "modernize" a non-critical asset would still be non-critical. It is left up to the Responsible Entity to determine if the newly built asset is a Critical Asset based on its impact to the reliability of the BES. Similarly, a Cyber Asset might be installed within an Electronic Security Perimeter that is not determined to be a Critical Cyber Asset.		
American Electric Power	Yes	AEP believes that there should be a statement in the standard providing a reference to the implementation plan and that the implementation plan be included in an appendix of the standard.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		

Organization	Yes or No	Question 12 Comment
City of Tallahassee (TAL)	Yes	I am for eliminating stand alone documents, although this incorporation can be made in Version 3, since you have stated one will be done for the more contentious issues.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Kansas City Power & Light	Yes	This seems like the most logical place to put those requirements. Otherwise we'll end up with Standards that have to be cross-referenced against multiple sets of documents.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Manitoba Hydro	Yes	Implementation plans which expire should be stand-alone documents from the standards. On-going implementation plans should be incorporated into the standards to create self-contained standards.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Old Dominion Electric Cooperative	Yes	I agree with including this information in the standards so everyone, user and Region, understands what is required. Leaving it in a stand alone document might allow for FERC to unilaterally change the implementation timeframe without stakeholder input. I hate to have to revise the CIP standards again, but this is important.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.		
Pepco Holdings, Inc - Affiliates	Yes	In response to the CSO706 SDT question, we agree that the implementation plan for newly identified Critical Cyber Assets should be incorporated into the cyber security standard and believe that it should be included as part of CIP-002-1.
Response: The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider		

Organization	Yes or No	Question 12 Comment
incorporating the implementation plan into the standards in a subsequent revision.		
Ameren	Yes	
American Transmission Company	Yes	
Applied Control Solutions, LLC	Yes	
BC Transmission Corporation	Yes	
Consolidated Edison Company of New York, Inc.	Yes	
Consumers Energy Company	Yes	
Deloitte & Touche, LLP	Yes	
Detroit Edison Company	Yes	
Duke Energy	Yes	
Dynegy	Yes	
Electric Market Policy	Yes	
Exelon	Yes	
ISO New England Inc	Yes	
Luminant Power	Yes	

Organization	Yes or No	Question 12 Comment
MidAmerican Energy Company	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Northeast Power Coordinating Council	Yes	
Northern Indiana Public Service Company	Yes	
Oncor Electric Delivery LLC	Yes	
Orange and Rockland Utilities Inc.	Yes	
PacifiCorp	Yes	
PPL Corporation	Yes	
Southern California Edison Company	Yes	
Southern Company	Yes	
Tampa Electric Company	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	

Organization	Yes or No	Question 12 Comment
WECC Reliability Coordination	Yes	
Xcel Energy	Yes	

13. Do you agree that the Phase 1 improvements addresses the **time-sensitive FERC Order directives**? If not, please explain.

Summary Consideration:

Several of the stakeholders asked for a clarification as to the intention of the phrase "shall make available" that is included in measures for each standard and whom an Entity is supposed to make documents available to. The SDT clarified that the phrase, “shall make available” means that the responsible entity must allow the Compliance Enforcement Authority to see the evidence for compliance, and be “made available” for review.

A few of the stakeholders expressed concern that the change from a three year retention for documents to a non-specific period will provide additional burden to the compliance process. The SDT responded that the data retention periods for the standard requirements are specified in the standards. The Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit plus all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.

Several stakeholders expressed concern that the new effective date for the CIP standards goes above the requirements listed in FERC Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans. The Standards Drafting Team reviewed the requirement and confirmed that the six to nine month implementation plan is reasonable and supports the new effective date for the CIP standards.

One stakeholder expressed concern that the Phase 1 revisions to the CIP standards are moving the standards away from "Critical Infrastructure Protection" and towards "Cyber Infrastructure Protection”. The Standard Drafting Team confirmed that it is focused on the cyber security aspects of critical infrastructure protection, a priority reflected in the SDT 706 SAR and is driven by national security concerns about the adequacy of the industry's cyber security efforts as stated by Congressional Committees, FERC, and the new Obama Administration.

Many stakeholders expressed concerned about the removal of the “reasonable business judgment” language from the CIP standards. However, this was done in accordance with FERC Order 706. The definition of the Technical Feasibility Exception Process should address the concerns regarding the removal of the reasonable business judgment and acceptance of risk language from the standards.

The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The Phase 1 revisions to the CIP-002 through CIP-009 standards were focused on the high priority issues raised by FERC in CSO 706 and the industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent Phases of the CIP standards.

Organization	Yes or No	Question 13 Comment
MidAmerican Energy Company	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards. The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.		
MRO NERC Standards Review Subcommittee	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards. The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.		
PacifiCorp	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards. The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.		

Organization	Yes or No	Question 13 Comment
Pepco Holdings, Inc - Affiliates	No	1. We understand that the SDT is proposing that Technical Feasibility Exceptions (TFE) Process (i.e. exception approval process) be modeled after the existing Self-Report and Mitigation Plan processes in the Compliance Monitoring and Enforcement Program (CMEP) which would require TFE review by the Regional Entity and NERC to assess the impact to the BES and then approve or not approve the exception. We also understand that as part of the NERC TFE approval process a mitigation plan would need to be submitted to the Regional Entity/NERC and completed for compliance. We understand that the Standards Drafting Team (SDT) is proposing that the TFE process be done through the NERC Rules of Procedure update process rather than through the standards process. Is it the intent of the SDT is to keep the TFE process outside of the compliance process (i.e., TFE requirement as part of the NERC Rules of Procedures)? 2. The existing Self-Report and Mitigation Plan process is for self-reporting and remedying a potential non-compliance. Is the intent of modeling the existing Self-Report and Mitigation Plan for the TFE process because the SDT considers Technical Feasibility Exceptions as non-compliance to the CIP standards? It was our understanding that TFEs are not a compliance issue. The existing FAQs state: Technical feasibility refers only to engineering possibility and is expected to be a "can/cannot" determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by the Responsible Entity. The Responsible Entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf 3. We believe that the TFE process needs to be included in the standards as well (e.g. CIP-003-2 R3). If the TFE is not coupled to the Standards (e.g. requirement to submit to RE and NERC for approval) we have concerns that there may be unintended gaps or conflicts. (i) For example what happens if a Registered Entity in following CIP-003-2 R3 (Exceptions) has a technical exception approved by the Sr. Manager but by a de-coupled TFE process NERC does not approve the exception? The Registered Entity is in compliance with the Standard but not with the TFE approval process. Would failure of a TFE procedure be considered non-compliance and therefore subject to fines? (ii) Another example of a potential gap or conflict is there could be conflicting effective dates of the standards and the TFE process (i.e. the requirement to submit to NERC for approval) if these are not linked together. (iii) Timing of the approvals by NERC could also create a gap or conflict. (iv) We encourage the SDT drafting team to consider including the requirement of RE/NERC review in the standards. The detailed process and procedures could be separate.

Organization	Yes or No	Question 13 Comment
		(v) Finally we believe that the SDT needs to identify how the RE and/or NERC will perform the assessment of a TFE request on the impact to the BES (e.g. engineering judgement, load flow studies, stability studies,...) and identify the parameters that would be considered an approved exception versus an unapproved exception. 4. We understand and agree that NERC has the right to review TFE information and evidence of compliance but providing this information/data offsite may be considered a violation to the CIP requirement(s) and at the very least is a potential risk because if this information is compromised could show vulnerabilities to Critical Cyber Assets at a given Registered Entity. The confidentiality and security of the data/information needs to be considered. Potential options could include: • NERC could review information over a secure communication channel without NERC keeping the sensitive information
Response: 1. The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk. 2. Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard. 3. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 4. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
San Diego Gas and Electric Co.	No	While the Standards Drafting Team has done a great job overall incorporating many of the issues raised in FERC Order 706 FERC, there appears to be two issues identified by FERC in Order 706 that have not been addressed by the Standards re-write team in these first revisions.

Organization	Yes or No	Question 13 Comment
		FERC Order 706 directed in Paragraph 88 that features such as enhanced conditions on technical feasibility exceptions and oversight of critical asset determinations for CIP-002 are too important to the protection of the Bulk-Power System to wait until the 2009-2010 time period for the process to start. But no substantial modifications for CIP-002 in these areas are included from the SDT. In addition, FERC Order 706, in Paragraph 90, also directed the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule. This doesn't appear to have been completed by the SDT as a first priority.
Response: In Paragraph 88, the Commission ordered revisions to the CIP standards not be delayed until completion of the Version 1 standards Implementation Plan, and specifically cited the CIP-002-1 and Technical Feasibility Exceptions (TFE) as priority revisions. The Commission at Paragraph 253 adopted the NOPR proposal requiring the ERO to provide additional guidance as to the features and functionality of an adequate risk-based assessment methodology, while leaving to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. The NERC Critical Infrastructure Protection Committee is in the process of developing specific Guidelines to address this requirement. The SDT believes the development of the Critical Asset and Critical Cyber Asset Identification Guidelines currently underway address the immediate concerns of the Commission. In addition, the SDT will be examining the entire risk management framework. Due to the complexity of this issue, the SDT decided to address risk management and its impact on CIP-002 early in Phase 2 in order to not delay the time-critical modifications directed elsewhere in the Final Order. The Commission at Paragraph 178 directed the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards. NERC Staff, with consultation with the SDT, has begun to develop a process for handling Technical Feasibility Exceptions (TFE) that is modeled after the existing self-report of non-compliance with mitigation plan process, as described in the NERC Rules of Procedure (ROP) Appendix 4C. The TFE process is not a "requirement" of a "standard" - it is a process for meeting requirements in standards. The TFE process is considered to be a compliance issue, although it is anticipated to be a way of being "compliant" with a standard in the event that an entity cannot meet the specific requirements of the standard. Because the TFE process is a compliance process, not development of requirements, it is outside the charter of the SDT. Therefore, the TFE process development and approval will be moving away from a direct SDT effort, to follow the established process for modifying the NERC Rules of Procedure (ROP). As such, the SDT will not have a formal role in continued development of the process. The established ROP update process includes public comment and stakeholder input (including continued input from the SDT).		
Luminant Power	No	Luminant thanks the Standards Drafting Team for their work addressing improvements to the NERC CIP Standards CIP-002 through CIP-009. As indicated by our "yes" responses to the comment form, in general Luminant agrees with the drafting team regarding the phased approach, implementation plan and the changes to address the time-sensitive issues from the FERC Order. However, on each

Organization	Yes or No	Question 13 Comment
		standard the drafting team changed the language under the Data Retention sections 1.4.1 and 1.4.2. Luminant agrees with the intent of the changes but does not believe the language provides sufficient clarity. Luminant respectfully submits the following suggested language for the aforementioned data retention sections on each standard. 1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 for the current calendar year and the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation. The Responsible Entity shall keep documentation required by the Compliance Enforcement Authority for an investigation for one year after Compliance Enforcement Authority notice to the Responsible Entity that the investigation is completed.1.4.2 The Compliance Enforcement Authority and the Responsible Entity shall each retain all requested and submitted audit records from the most recent audit.
Response: The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.		
CenterPoint Energy	No	See responses above to Q5, Q7, and Q8. In addition, the SDT changed the data retention wording in CIP-002 through CIP-009 such that "the Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records." CenterPoint Energy believes the retention time should be more defined and proposes adding "until the next scheduled audit" to make it clear that data retention is on a rolling basis.

Organization	Yes or No	Question 13 Comment
Response: The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.		
Encari	No	FERC provided directives on nearly all of the current requirements and guidance to include further requirements. The identification of what to modify in a time-sensitive manner was not open for public comment. We recognize the need to act swiftly to protect the assets; however, assurances also need to be made to protect system reliability. As an example, we feel that further clarifications around how to select critical assets and critical cyber assets would have provided a greater impact on the process and recommend that a public comment period be opened for the current draft guidelines. Therefore we recommend providing public comment periods to help the selection process of which FERC directives to introduce in the next phase of changes.
Response: The Standards Drafting Team agrees that there are a variety of pressing needs such that a proritization process would be helpful. Once the time sensitive issues have been identified, the next step includes a discussion about the phased implementation approach to all of the FERC recommendations, while also considering industry needs.		
Applied Control Solutions, LLC	No	NIST Framework needs to be addressed NOW!
Response: The Standards Drafting Team will consider the NIST risk management framework in future revisions of the standards.		
US Bureau of Reclamation	No	The revisions are moving these standards away from "Critical Infrastructure Protection" towards "Cyber Infrastructure Protection." We believe this move strays from the original intent of Critical Infrastructure Protection as defined by the initial requirements. By focusing solely on the Cyber aspect, many important aspects of critical infrastructure protection will be lost. We reject any efforts to modify CIP from Critical Infrastructure Protection to Cyber Infrastructure Protection.

Organization	Yes or No	Question 13 Comment
Response: The Standard Drafting Team is focused on the cyber security aspects of critical infrastructure protection, a priority reflected in the SDT 706 SAR and driven by national security concerns about the adequacy of the industry's cyber security efforts as stated by Congressional Committees, FERC, and the new Obama Administration. Nonetheless, the SDT agrees that there is a critical need to address non-cyber critical infrastructure issues. If the commenter believes such an effort is warranted, we would recommend the submission of a SAR to specify the applicable issues.		
Progress Energy	Yes	1) Overall comment - PE recommends the removal of "Reasonable business judgment" be replaced with the use of "good utility practice" as defined by FERC. 2) Overall comment - Section D – Data Retention – It is not practical to leave data retention period totally open ended at the sole discretion of the Compliance Enforcement Authority, there should at least be a capped limit, PE recommends a maximum of 3-years to allow time between audits.
Response: 1) The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk. **2)** The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.		
Ameren	Yes	Would like to see a clarification on what is intended by phrase "shall make available" that is included in measures for each standard and whom an entity is supposed to make documents available to. The change from a three year retention for documents to a non-specific period will provide additional burden to the compliance process, since the region will have an arbitrary time length assigned per specific incident.
Response: The phrase, "shall make available" means that the responsible entity must allow the Compliance Enforcement Authority to see the evidence. The evidence is made available to the Compliance Enforcement Authority. The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance		

Organization	Yes or No	Question 13 Comment
Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator, and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.		
American Electric Power	Yes	As described above and following, AEP believes that there are a number of concepts that need to be discussed and clarified in the standards. 1) AEP requests clarification be added about changes to Data Retention item 1.4.2. NERC reference materials suggest that the Compliance Enforcement Authority is solely responsible for keeping the last audit records. AEP does not believe that expanding the role of the Registered Entity, beyond that in any other standard, to include keeping audit documents is necessary or appropriate. However, there may be circumstances where confidential underlying data concerning critical infrastructure should only be retained only by the Registered Entity, but, even in such circumstances, auditing records should solely be retained under requirement by the Compliance Inforcement Authority. 2) Technical consideration should be given to determining the response to the "Compliance Monitoring Period and Reset Time Frame" section. The drafting team reference guide has suggested time periods aligning with audits cycles and less than monthly reset time frames. The response that it is not applicable does not appear consistent. 3) Lastly, item M1 under Measures has inadvertently dropped the "The" while the remaining M2 - M4 do contain "The" at the beginning of each sentence. In some of the following CIP standards, it is presented correctly, and, in others, it is not aligned within the M1 item.
Response: 1) The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept. The language of 1.4.2 indicates that the Compliance Enforcement Authority “in conjunction with” the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.		

Organization	Yes or No	Question 13 Comment
		The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator, and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity. 2) The compliance monitoring period and reset timeframe were linked to an older version of the sanctions table, and have no relevance to the sanctions table currently in use. Until the Reliability Standards Development Procedure is updated, we cannot remove this heading from the standard template; until then all drafting teams are placing the phrase, "not applicable" under the heading, "Compliance Monitoring Period and Reset Time Frame" in the standard. 3) The SDT is not able to locate the specific reference in the Measures associated with this comment. We will attempt to address such remaining issues in future relreases of the CIP standards. Please resubmit your comment as appropriate if they have not been addressed at that time.
Southern California Edison Company	Yes	SCE hereby submits these additional general comments and questions (not related to or in response to Question 13): 1. What is the approval process for Violation Severity Levels? Will they be part of the standards? Will they be circulated for comment as part of the approval process? 2. In the Data Retention section of each Standard, a retention period is not specified for audit records. What is the retention period?
Response: 1) The Violation Severity Levels (VSLs) for Version 1 of the CIP Standards (CIP-002-1 through CIP-009-1) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team. The VSLs for Version 2 of the CIP Standards (CIP-002-2 through CIP-009-2) associated with the changes being proposed by the Standards Drafting Team for this project are currently being coordinated with the other Standards Drafting Team and will be posted for Industry Comment. The schedule for doing so is currently unknown. 2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control		

Organization	Yes or No	Question 13 Comment
over these records. Most other records will be retained by the Compliance Enforcement Authority.		
ISO New England Inc	Yes	1) We agree with the removal of "reasonable business judgment" and "acceptance of risk." 2) GENERAL COMMENT: As a general matter, NERC needs to explain how it plans on enforcing these standards. This is critical, because NERC is not defining what cyber-security practices are, in fact, acceptable. Therefore, if a company establishes a "high bar for its internal programs (e.g., training employees), and does not meet its own business practices, it can be fined by NERC. By contrast (and depending on how the standards are enforced) companies that set "low bars" for its internal programs will escape penalty. NERC could inadvertently, through its compliance and enforcement policy, incent companies to establish "lowest common denominator" practices.
Response: 1) The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk. 2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
City of Tallahassee (TAL)	Yes	I may not agree with all changes but they do address the FERC Order directives, even though by making these directives, they violate the ANSI approved process that they have stated NERC is required to follow.
Response: Comments regarding the ANSI process are outside the scope of the SDT to address.		
FirstEnergy Corp	Yes	For the most part we agree with the improvements except for our previous comments in questions 3, 10 and 11. Also, we offer the following additional suggested improvements: 1) CIP-002-2 R3 - The phrase "automatic generation control" should be capitalized since it is a NERC defined term. 2) CIP-003 M1 - The SDT should consider removing the second sentence "Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in

Organization	Yes or No	Question 13 Comment
		Requirement R1.2" since the language in the first sentence already covers the necessary measure. 3) CIP-005 R2.4 - The word "strong" should be removed since it is not clearly defined and measurable.CIP-007 - R2,R3,R5 - The word "establish" should be removed consistant with the other CIP standards. All that should be required is to "implement and document".- R5.1.2 - Replace "establish" with "have".- R7 - Replace "establish" with "document. 4) CIP-009 - The first sentence in "Sec. B Requirements" which states "The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:" is not necessary and should be removed consistant with the other CIP revisions. 5) FAQ Document - Is the SDT considering changes to the FAQ document to align with these proposed changes to the standards? Or is the FAQ document not a "living" document and was only to be used for the version 1 standards development? 6) Regarding measures in CIP-002 through CIP-009, the drafting team should consider revising the measures to include some guidance on the types of evidence or documentation that a responsible entity should and/or could have to demonstrate compliance. 7) Throughout the standards the phrases "at least" and "at a minimum" are used and we feel that they are unnecessary. It is already understood that the standard requirements are the minimum expectations. 8) Throughout the standards we suggest the SDT add the VRFs for each main requirement. 9) Lastly, it would be appreciated if the SDT would use underlining in addition to the blue colored text to reflect inserted text for readability of black-n-white printed/copied material.

Response:

1) The term automatic generation control is not capitalized since it has broad applicability including the official NERC definition of Automatic Generation Control.

2) CIP-003 M1 is meant to indicate how compliance to Requirements R1 and R1.2 will be met. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

3) These types of issues will be further addressed in later phases of the CIP Standards. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

4) These types of issues will be further addressed in later phases of the CIP Standards. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

5) These types of issues will be further addressed in later phases of the CIP Standards. The SDT suggests that you review the changes

Organization	Yes or No	Question 13 Comment
proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 6) These types of issues will be further addressed in later phases of the CIP Standards. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 7) These types of issues will be further addressed in later phases of the CIP Standards. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 8) The Violation Risk Factors (VRFs) will be addressed in future phases of the CIP Standards. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. 9) We will do our best to address this issue in future releases of the standards for comment.		
Northern Indiana Public Service Company	Yes	Not sure if the question pertains to the CIP draft modifications or the proposed implementation schedule.
Response: The Question pertains to both items.		
American Transmission Company	Yes	
Austin Energy	Yes	
BC Transmission Corporation	Yes	
Bonneville Power Administration	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Consolidated Edison Company of New York, Inc.	Yes	We agree that Phase 1 addresses the time-sensitive FERC Order directives to remove "reasonable business judgment" and "acceptance of risk".

Organization	Yes or No	Question 13 Comment
Response: Thank you for your comment.		
Consumers Energy Company	Yes	
Deloitte & Touche, LLP	Yes	
Detroit Edison Company	Yes	
Duke Energy	Yes	
Dynegy	Yes	
Electric Market Policy	Yes	
Exelon	Yes	
Kansas City Power & Light	Yes	
KEMA	Yes	
Manitoba Hydro	Yes	
Northeast Power Coordinating Council	Yes	We agree with the removal of "reasonable business judgment" and "acceptance of risk".
Response: Thank you for your comment.		
Old Dominion Electric Cooperative	Yes	

Organization	Yes or No	Question 13 Comment
Oncor Electric Delivery LLC	Yes	
Ontario IESO	Yes	
Orange and Rockland Utilities Inc.	Yes	
PPL Corporation	Yes	
Southern Company	Yes	
Standards Review Committee of ISO/RTO Council	Yes	
Tampa Electric Company	Yes	
TransAlta Centralia Generation, LLC	Yes	
TVA	Yes	
United Illuminating Company	Yes	
WECC Reliability Coordination	Yes	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool and Pre-ballot Window
March 3–April 1, 2009

Now available at: https://standards.nerc.net/BallotPool.aspx

Revisions to Cyber Security Standards CIP-002-1 through CIP-009-1 (Project 2008-06)

The Cyber Security Standard Drafting Team (Project 2008-06) has posted its revisions to cyber security standards CIP-002-1 through CIP-009-1 for a 30-day pre-ballot review. Registered Ballot Body members may join the ballot pool to be eligible to vote on these standards revisions **until 8 a.m. EDT on April 1, 2009**. The posting includes associated implementation plans for the standards.

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once balloting begins, ballot pool members are prohibited from using the ballot pool list server.) The list server for this ballot pool is: bp-2008-06_CIP_2-9_Rev_in

Project Background

The Cyber Security Standard Drafting Team has been assigned the responsibility of revising the cyber security standards as follows:

- ensure the standards conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure,
- address the directed modifications identified in FERC Order 706, and
- consider other cyber-related standards, guidelines, and activities.

The drafting team subdivided its work into multiple phases, with "Phase I" (the current phase) focused on addressing near term directives in FERC Order 706. The most significant of these revisions addresses the directive to remove references to "reasonable business judgment" before compliance audits begin in 2009. All issues that will require significant industry debate were deferred to later phases of the project to ensure that the FERC imposed deadline for removing "reasonable business judgment" can be met.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date	To be determined.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

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

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date	To be determined.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

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

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its ~~dated~~ list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its ~~dated~~ list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its ~~dated~~ approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~-~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (~~Under Development by the CIP VSL Drafting Team~~To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before

compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

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

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before

compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

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

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, ~~business phone~~ and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (~~Under Development by the CIP VSL Drafting Team~~To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-2

3. Purpose: Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);

- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program**.** Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

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

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

3. **Purpose:** Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-004-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and~~,~~ maintain~~, document and implement~~ a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);

- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain~~, document and implement~~ an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, ~~reviewed~~ and shall be updated ~~as~~ whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (~~Under Development by the CIP VSL Drafting Team~~To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

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

2. Number: CIP-005-2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity.	

		Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

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

2. Number: CIP-005-2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain ~~and implement~~ a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

M1. The Responsible Entity shall make available ~~dated documents~~ documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available ~~dated~~ documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available ~~dated~~ documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available ~~dated~~ documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available ~~dated~~ access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (~~Under Development by the CIP VSL Drafting Team~~To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a	

		responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-2

3. Purpose: Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-006-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets

2. **Number:** CIP-006-2

3. **Purpose:** Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-006-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain~~, and implement~~ a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement ~~R3~~ R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~.~~

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Postd for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that	

		Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Postd for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (~~Under development by the CIP VSL Drafting Team~~To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk.	

		Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-2

3. Purpose: Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-2

3. Purpose: Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its ~~dated~~ Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (~~Under Development by the CIP VSL Drafting Team~~To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-2

3. Purpose: Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Conduct initial ballot	April 2–11, 2009
2. Post response to comments on first ballot	April 20–May 12, 2009
3. Conduct recirculation ballot	May 13–22, 2009
4. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-2

3. Purpose: Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:~~

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its ~~dated~~ recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its ~~dated~~ records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its ~~dated~~ documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its ~~dated~~ documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its ~~dated~~ documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (~~Under development by the CIP VSL Drafting Team~~To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-1~~1~~2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-002-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-002:~~

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — ~~A~~ The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of

the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:~~

M1. ~~The~~ Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. ~~The~~The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 ~~Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor~~None.

2. ~~Levels of Non-Compliance~~Violation Severity Levels (To be developed later.)

~~**2.1 Level 1:** The risk assessment has not been performed annually.~~

~~**2.2 Level 2:** The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.~~

~~**2.3 Level 3:** The list of Critical Assets or Critical Cyber Assets does not exist.~~

~~**2.4 Level 4:** The lists of Critical Assets and Critical Cyber Assets do not exist.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~1~~2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~.~~ ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-003:~~

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, ~~business phone, business address,~~ and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures~~, or a statement accepting risk~~.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or ~~-~~delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, ~~business phone~~ and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements~~ Responsible Entity shall make available documentation of ~~Standard CIP-003:~~

M1. ~~Documentation of the Responsible Entity's~~its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. ~~Documentation~~ The Responsible Entity shall make available documentation of the assignment of, and changes to, ~~the Responsible Entity's~~its leadership as specified in Requirement R2.

M3. ~~Documentation of the Responsible Entity's~~ The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. ~~Documentation of the~~The Responsible ~~Entity's~~Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible ~~Entity's~~Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.~~

~~**2. Levels of Noncompliance**~~

~~**2.1. Level 1:**~~

~~**2.1.1** Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,~~

~~**2.1.2** Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,~~

~~**2.1.3** An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.~~

~~**2.2. Level 2:**~~

~~**2.2.1** A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,~~

~~2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,~~

~~2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,~~

~~2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.~~

~~2.3. Level 3:~~

~~2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,~~

~~2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,~~

~~2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.~~

~~2.4. Level 4:~~

~~2.4.1 No cyber security policy exists; or,~~

~~2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,~~

~~2.4.3 No documented change control and configuration management process exists.~~

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to	

		include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-1~~2~~

3. Purpose: Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-004-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-004:~~

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain~~, and document~~ a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

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

R2. Training — The Responsible Entity shall establish, document, implement, and maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the. The cyber security training program shall be reviewed annually, at a minimum, and update asshall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days ofprior to their being granted such authorization.access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program within thirty days ofprior to such personnel being granted such access. Such except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:~~

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. ~~Documentation of the~~The Responsible ~~Entity's~~Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. ~~Documentation~~The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. ~~Documentation~~The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.~~

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~**2.1.1** Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,~~

~~**2.1.2** Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,~~

~~**2.1.3** Personnel risk assessment program exists, but documentation of that program does not exist; or,~~

~~**2.1.4** List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.~~

~~**2.1.5** One personnel risk assessment is not updated at least every seven years, or for cause; or,~~

~~**2.1.6** One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.~~

~~2.2. Level 2:~~

~~**2.2.1** Awareness program does not exist or is not implemented; or,~~

~~**2.2.2** Training program exists, but does not address the requirements identified in Standard CIP-004; or,~~

~~**2.2.3** Personnel risk assessment program exists, but assessments are not conducted as required; or,~~

~~2.2.4 One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.~~

~~2.3. Level 3:~~

~~2.3.1 Training program exists, but has not been reviewed and updated at least annually; or,~~

~~2.3.2 A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,~~

~~2.3.3 List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.~~

~~2.4. Level 4:~~

~~2.4.1 No documented training program exists; or,~~

~~2.4.2 No documented personnel risk assessment program exists; or,~~

~~2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel termination for cause…”	03/24/06
1	06/01/06	D.2.1.4 — Change “access control rights” to “access rights.”	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to	

		clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to “Critical Cyber Assets”. Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

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

2. Number: CIP-005-~~1~~2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations.~~Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-005:~~

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003~~,~~-2; Standard CIP-004-2 Requirement R3~~,~~; Standard CIP-005-2 Requirements R2 and R3~~,~~; Standard CIP-006 ~~Requirements R2 and~~ -2 Requirement R3~~,~~-; Standard CIP-007~~,~~-2 Requirements R1 and R3 through R9~~,~~; Standard CIP-008~~,~~-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; ~~and,~~

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-005.~~ Responsible ~~entities may document controls either individually or by specified applicable grouping.~~

M1. ~~Documents~~ Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. ~~Documentation~~The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. ~~Documentation~~The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. Access The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1. Compliance Enforcement Authority

1.1.1 Regional Reliability Organizations Entity for Responsible Entities.

1.1.1 NERC that do not perform delegated tasks for their Regional Reliability Organization Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The compliance monitor Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records for three years. and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior

manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

~~2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,~~

~~2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,~~

~~2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-1~~2~~

3. Purpose: Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~.~~ ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~ -2.

4. Applicability:

4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-006-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-006:~~

R1. Physical Security Plan — The Responsible Entity shall ~~create~~document, implement, and maintain a physical security plan, approved by ~~a~~ the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. ~~Processes to ensure and document that all~~ All Cyber Assets within an Electronic Security Perimeter ~~also~~ shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the

Responsible Entity shall deploy and document alternative measures to control physical access to ~~the Critical~~such Cyber Assets.

R1.2. ~~Processes to identify all~~Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. ~~Procedures for the appropriate~~Appropriate use of physical access controls as described in Requirement ~~R3~~R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. ~~Procedures for reviewing~~Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. ~~Procedures for~~Continuous escorted access within the ~~physical security perimeter~~Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. ~~Process for updating~~ Update of the physical security plan within ~~ninety~~thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the ~~physical security perimeter~~Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets ~~used in the~~that authorize and/or log access ~~control and monitoring of~~to the Physical Security Perimeter(s~~)~~), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall ~~be~~:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003~~,~~-2; Standard CIP-004-2 Requirement R3~~,~~; Standard CIP-005-2 Requirements R2 and R3~~,~~; Standard CIP-006 ~~Requirement R2 and R3,~~-2 Requirements R4 and R5; Standard CIP-007~~,~~-2; Standard CIP-008-2; and Standard CIP-009-2.

~~**R1.9.** Process for ensuring that the physical security plan is reviewed at least annually.~~

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

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

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3R4, R5, and R4R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance withResponsible Entity shall make available the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. DocumentationThe Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2R4.

M5. DocumentationThe Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R3R5.

M6. DocumentationThe Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R4R6.

M7. AccessThe Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R5R7.

M8. DocumentationThe Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R6.R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1. Compliance Enforcement Authority

1.1.1 Regional Reliability OrganizationsEntity for Responsible Entities.

1.1.1 NERC that do not perform delegated tasks for their Regional Reliability OrganizationEntity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R5R7 and R6R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The compliance monitorCompliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records for three calendar years.and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

2. Violation Severity Levels of Noncompliance

2.1. Level 1:

2. The physical security plan exists, but has not been updated within ninety calendar days of a modification to(Under development by the plan or any of its components; or,CIP VSL Drafting Team)

3.1.1 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

3.1.2 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

3.1.3 Physical access logs are retained for a period shorter than ninety days; or,

3.1.4 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

3.1.5 One required document does not exist.

3.2. Level 2:

3.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

3.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

3.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

3.2.4 More than one required document does not exist.

3.3. Level 3:

~~3.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,~~

~~3.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~3.3.3 No logs of monitored physical access are retained.~~

~~3.4. Level 4:~~

~~3.4.1 No physical security plan exists; or,~~

~~3.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~3.4.3 No maintenance or testing program exists.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance	

		Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~1~~2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):~~

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service

packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish ~~and~~ , document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish ~~and~~ , document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~thirty calendar days of the change being completed.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:~~

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. ~~Documentation~~The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. ~~Documentation~~The Responsible Entity shall make available documentation and records of ~~the Responsible Entity's~~its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. ~~Documentation~~The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.~~

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~**2.1.1** System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or~~

~~**2.1.2** One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,~~

~~**2.1.3** One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,~~

~~**2.1.4** Any one of:~~

- ~~Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,~~
- ~~A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,~~
- ~~Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.~~

~~2.2. Level 2:~~

~~2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.3. Level 3:~~

~~2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4. Level 4:~~

~~2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4.3 No logs exist.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-1~~2~~

3. **Purpose:** Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. **Applicability**

   4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional ~~Reliability Organizations~~Entity.

   4.2. The following are exempt from Standard CIP-008-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. **Effective Date:** ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-008:~~

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident ~~Response~~response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of ~~incident~~Cyber Security Incident response teams, ~~incident~~Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ~~–~~ ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ~~–~~ ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the ~~incident~~Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of CIP-008:~~

M1. ~~The~~ Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. ~~All~~The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.~~

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

~~2. Levels of Noncompliance~~

~~**2.1. Level 1:** A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.~~

~~**2.2. Level 2:**~~

~~**2.2.1** A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,~~

~~**2.2.2** A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,~~

~~**2.2.3** Records related to reportable Cyber Security Incidents were not retained for three calendar years.~~

~~**2.3. Level 3:**~~

~~**2.3.1** A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,~~

~~**2.3.2** A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.~~

~~**2.4. Level 4:** A Cyber Security Incident response plan does not exist.~~

2. **Violation Severity Levels (To be developed later.)**

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-~~1~~2

3. Purpose: Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional ~~Reliability Organizations~~Entity

4.2. The following are exempt from Standard CIP-009-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-009:~~

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:~~

M1. ~~Recovery~~Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. ~~Records~~The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. ~~Documentation of~~ The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. ~~Documentation~~The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. ~~Documentation~~The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.34.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.34.2 The Compliance ~~Monitor~~Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.~~

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,~~

~~2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.~~

~~2.2. Level 2:~~

~~2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,~~

~~2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.~~

~~2.3. Level 3:~~

~~2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,~~

~~2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.~~

~~2.4. Level 4:~~

~~2.4.1 No recovery plan(s) exist; or,~~

~~2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Modified Standards

The following standards have been modified:
CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

Red-line versions of the above standards are posted with this Implementation Plan. When these modified standards become effective, the prior versions of these standards and their Implementation Plan are retired.

Compliance with Standards

Once these standards become effective, the responsible entities identified in the Applicability section of the standard must comply with the requirements. These include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.

Proposed Effective Date

The proposed effective date for these modified standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters) after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Modified Standards

The following standards have been modified:
CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

Red-line versions of the above standards are posted with this Implementation Plan. When these modified standards become effective, the prior versions of these standards and their Implementation Plan are retired.

Compliance with Standards

Once these standards become effective, the responsible entities identified in the Applicability section of the standard must comply with the requirements. These include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.

Proposed Effective Date

The proposed effective date for these modified standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters) after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan identifies the schedule for becoming compliant with the requirements of NERC Standards CIP-003-2 through CIP-009-2 and their successor standards, for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed.

This Implementation Plan specifies only a 'Compliant' milestone. The Compliant milestone is expressed in this Implementation Plan table (Table 2) as the number of months following the designation of the newly identified asset as a Critical Cyber Asset, following the requirements of NERC Standard CIP-002-2 or its successor standard.

For some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as '0' herein. For other requirements, the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date. These are annotated as *existing*.

In all cases where a milestone for compliance is specified (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the milestone listed in this Implementation Plan. Where the milestone assumes prior compliance (i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones.

There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.

Implementation Schedule

There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:

1. A Cyber Asset becomes the *first identified* Critical Cyber Asset at a responsible Entity. No existing CIP compliance program for CIP-003 through CIP-009 is assumed to exist at the Responsible Entity.
2. An existing Cyber Asset becomes subject to CIP standards, *not due to planned change*. A CIP compliance program already exists at the Responsible Entity.
3. A new or existing Cyber Asset becomes subject to CIP standards *due to planned change*. A CIP compliance program already exists at the Responsible Entity.

Note that the term 'Cyber Asset becomes subject to the CIP standards' applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

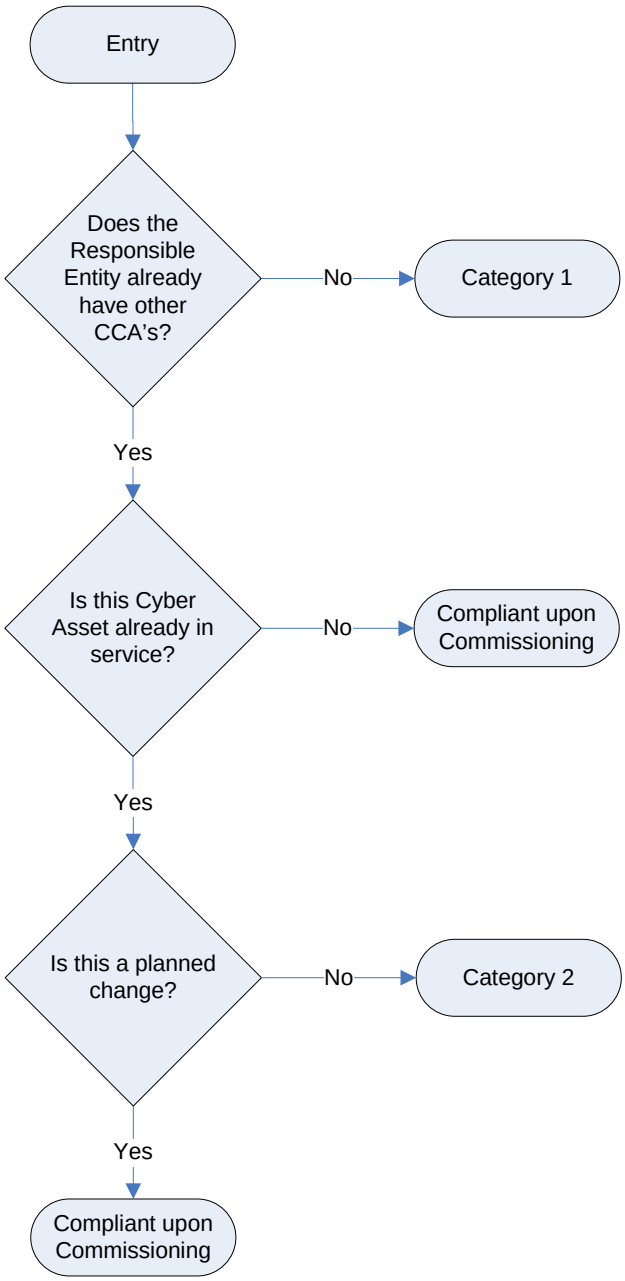

Figure 1: Category Selection Process Flow

The individual categories are distinguished as follows:

1. **Category 1**: A Responsible Entity that previously has undergone the CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-002-1 through CIP-009-1.) As such, it is presumed that the Responsible Entity has no previously established cyber security program in force. Table 3 also shall apply in the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.

2. **Category 2**: A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule, and now has added additional items to its Critical Cyber Asset list. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented. Since the Responsible Entity already has a CIP compliance program, it needs only to implement the CIP standards for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement.

   In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.

   In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.

   A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

3. **Compliant upon Commissioning**: When a Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

    a) 'Greenfield' construction of an asset that will be declared a Critical Asset upon its commissioning or activation (e.g., based on planning or impact studies).
    b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset.
    c) Planned addition of:
        i. a Critical Cyber Asset, or,
        ii. an other (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

    In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset where that Entity has an established CIP Compliance Program as required by an existing Implementation Schedule.

    This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.

    A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

    A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

    Since the assets must be compliant upon commissioning, no milestones are provided herein.

Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards.

As an example, Table 1 provides some sample situations, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Program:	
	No CIP Program (note 1)	Existing CIP Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset - never before in service and not a replacement for an existing Cyber Asset - added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[1] Compliance Schedule for Standards CIP-002-2 through CIP-009-2 or Their Successor Standards For Entities Registering in 2008 and Thereafter				
	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	**All Facilities**	**All Facilities**	**All Facilities**	**All Facilities**
CIP-002-2 Critical Cyber Assets or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-003-2 — Security Management Controls or its Successor Standard				
All Requirements Except R2	**BW**	**SC**	**C**	**AC**
R2	**SC**	**C**	**AC**	**AC**
Standard CIP-004-2 — Personnel & Training or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-005-2 — Electronic Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-006-2 — Physical Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-007-2 — Systems Security Management or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-008-2 — Incident Reporting and Response Planning or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-009-2 — Recovery Plans or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**

[1] The phase in of compliance in this table is identical to the phase in for CIP-002-1 through CIP-009-1 identified in Table 4 of the 2006 CIP Implementation Plan.

Implementation Plan for Cyber Security Standards CIP-003-~~1~~2-2 through CIP-009-~~1~~ 2 or Their Successor Standards

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan identifies the schedule for becoming compliant with the requirements of NERC Standards CIP-003-~~1~~ 2 through CIP-009-~~1~~ 2 and their successor standards, for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed.

This Implementation Plan specifies only a 'Compliant' milestone. The Compliant milestone is expressed in this Implementation Plan table (Table 2) as the number of months following the designation of the newly identified asset as a Critical Cyber Asset, following the requirements of NERC Standard CIP-002-~~1~~ 2 or its successor standard.

For some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as '0' herein. For other requirements, the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date. These are annotated as *existing*.

In all cases where a milestone for compliance is specified (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the milestone listed in this Implementation Plan. Where the milestone assumes prior compliance (i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones.

There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.

Implementation Schedule

There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:

1. A Cyber Asset becomes the *first identified* Critical Cyber Asset at a responsible Entity. No existing CIP compliance program for CIP-003 through CIP-009 is assumed to exist at the Responsible Entity.
2. An existing Cyber Asset becomes subject to CIP standards, *not due to planned change*. A CIP compliance program already exists at the Responsible Entity.
3. A new or existing Cyber Asset becomes subject to CIP standards *due to planned change*. A CIP compliance program already exists at the Responsible Entity.

Note that the term 'Cyber Asset becomes subject to the CIP standards' applies to all Critical Cyber Assets, as well as ~~non-critical~~other (non-critical) Cyber Assets within an Electronic Security Perimeter.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

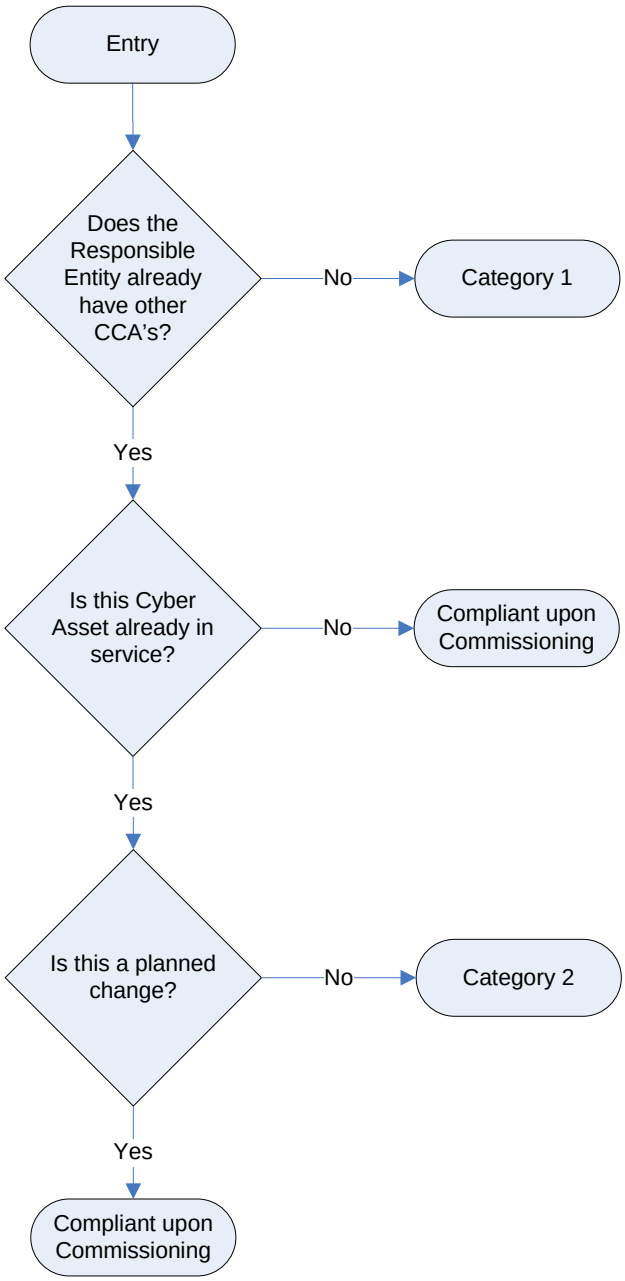

Figure 1: Category Selection Process Flow

The individual categories are distinguished as follows:

1. **Category 1**: A Responsible Entity that previously has undergone the CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-~~003~~002-1 through CIP-009-1.) As such, it is presumed that the Responsible Entity has no previously established cyber security program in force. Table 3 also shall apply in the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.

2. **Category 2**: A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule, and now has added additional items to its Critical Cyber Asset list. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented. Since the Responsible Entity already has a CIP compliance program, it needs only to implement the CIP standards for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement.

   In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.

   In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.

   A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

3. **Compliant upon Commissioning**: When a Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

    a) 'Greenfield' construction of an asset that will be declared a Critical Asset upon its commissioning or activation (e.g., based on planning or impact studies).
    b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security ~~perimeter~~Perimeter) associated with a previously identified Critical Asset.
    c) Planned a~~A~~ddition of:
        i. a Critical Cyber Asset, or,
        ii. an other (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

    In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset where that Entity has an established CIP Compliance Program as required by an existing Implementation Schedule.

    This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.

    A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

    A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

    Since the assets must be compliant upon commissioning, no milestones are provided herein.

Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards.

As an example, Table 1 provides some sample situations, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Program:	
	No CIP Program (note 1)	Existing CIP Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset - never before in service and not a replacement for an existing Cyber Asset - added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) ~~non-critical~~ asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	~~1~~*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	~~existing~~6 months
R5	24 months	6 months~~*existing*~~
R6	24 months	6 months~~*existing*~~
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18~~6~~ months
R3	24 months	~~6~~18 months
R4	24 months	~~6~~18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	~~0~~6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	~~0~~12 months
R3	24 months	~~0~~12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[1] Compliance Schedule for Standards CIP-002~~-1~~-2 through CIP-009~~-1~~-2 or Their Successor Standards For Entities Registering in 2008 and Thereafter				
	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	**All Facilities**	**All Facilities**	**All Facilities**	**All Facilities**
CIP-002~~-1~~-2 Critical Cyber Assets or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-003~~-1~~-2 — Security Management Controls or its Successor Standard				
All Requirements Except R2	**BW**	**SC**	**C**	**AC**
R2	**SC**	**C**	**AC**	**AC**
Standard CIP-004~~-1~~-2 — Personnel & Training or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-005~~-1~~-2 — Electronic Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-006~~-1~~-2 — Physical Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-007~~-1~~-2 — Systems Security Management or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-008~~-1~~-2 — Incident Reporting and Response Planning or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-009~~-1~~-2 — Recovery Plans or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**

[1] The phase in of compliance in this table is identical to the phase in for CIP-002-1 through CIP-009-1 identified in Table 4 of the 2006 CIP Implementation Plan.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Initial Ballot Window Open

April 1–10, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Revisions to Cyber Security Standards CIP-002-1 through CIP-009-1 (Project 2008-06)

An initial ballot window for revisions to cyber security standards CIP-002-1 through CIP-009-1 is now open **until 8 p.m. EDT on April 10, 2009.** The posting includes an associated implementation plan for the standards.

Project Background

The Cyber Security Standard Drafting Team has been assigned the responsibility of revising the cyber security standards as follows:

- ensure the standards conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure,
- address the directed modifications identified in FERC Order 706, and
- consider other cyber-related standards, guidelines, and activities.

The drafting team subdivided its work into multiple phases, with "Phase I" (the current phase) focused on addressing near term directives in FERC Order 706. The most significant of these revisions addresses the directive to remove references to "reasonable business judgment" before compliance audits begin in 2009. All issues that will require significant industry debate were deferred to later phases of the project to ensure that the FERC imposed deadline for removing "reasonable business judgment" can be met.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Revisions to Cyber Security Standards CIP-002-1 through CIP-009-1 (Project 2008-06)
Since at least one negative ballot was submitted with a comment, a recirculation ballot will be held. The recirculation ballot will be held after the drafting team responds to voter comments submitted during this ballot.

The initial ballot for for revisions to cyber security standards CIP-002-1 through CIP-009-1 ended April 10, 2009. The ballot results are shown below. The Ballot Results Web page provides a link to the detailed results.

Quorum: 91.90%
Approval: 84.06%

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Ballot Criteria
Approval requires both:

- A quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention; and
- A two-thirds majority of the weighted segment votes cast must be affirmative. The number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses.

Standards Development Process
The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results

Ballot Name:	Project 2008-06 CIP-002-1-CIP-009-1 Revisions_in
Ballot Period:	4/1/2009 - 4/10/2009
Ballot Type:	Initial
Total # Votes:	261
Total Ballot Pool:	284
Quorum:	**91.90 % The Quorum has been reached**
Weighted Segment Vote:	84.06 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	77	1	58	0.853	10	0.147	4	5
2 - Segment 2.	10	0.7	5	0.5	2	0.2	1	2
3 - Segment 3.	67	1	50	0.909	5	0.091	4	8
4 - Segment 4.	23	1	14	0.737	5	0.263	2	2
5 - Segment 5.	59	1	39	0.765	12	0.235	4	4
6 - Segment 6.	30	1	24	0.857	4	0.143	1	1
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	6	0.5	4	0.4	1	0.1	0	1
9 - Segment 9.	4	0.4	4	0.4	0	0	0	0
10 - Segment 10.	8	0.8	8	0.8	0	0	0	0
Totals	**284**	**7.4**	**206**	**6.221**	**39**	**1.179**	**16**	**23**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	ATCO Electric	Doug Smeall	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	

1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	View
1	CenterPoint Energy	Paul Rocha	Negative	
1	Central Maine Power Company	Brian Conroy	Negative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Alan L Cooke	Affirmative	
1	City Utilities of Springfield, Missouri	Jeff Knottek	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	E.ON U.S. LLC	Larry Monday	Abstain	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	View
1	Farmington Electric Utility System	Alan Glazner		
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	C. Martin Mennes	Abstain	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	JEA	Ted E. Hobson		
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	View
1	Kissimmee Utility Authority	Joe B Watson	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	Rodney Hawkins	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	Minnesota Power, Inc.	Carol Gerou	Affirmative	
1	National Grid	Manuel Couto	Affirmative	
1	Nebraska Public Power District	Richard L. Koch	Affirmative	
1	New Brunswick Power Transmission Corporation	Brian Scott	Affirmative	
1	New York Power Authority	Ralph Rufrano	Abstain	View
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	View
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Puget Sound Energy, Inc.	Catherine Koch	Affirmative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SaskPower	Wayne Guttormson	Negative	View
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	View
1	South Texas Electric Cooperative	Richard McLeon	Affirmative	
1	Southern California Edison Co.	Dana Cabbell	Negative	View
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Abstain	
1	Tampa Electric Co.	Thomas J. Szelistowski	Negative	View
1	Tennessee Valley Authority	Larry Akens	Negative	View
1	Transmission Agency of Northern California	James W. Beck	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	

1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Western Farmers Electric Coop.	Alan Derichsweiler	Affirmative	
1	Xcel Energy, Inc.	Gregory L. Pieper	Affirmative	
2	Alberta Electric System Operator	Anita Lee	Abstain	View
2	British Columbia Transmission Corporation	Phil Park	Affirmative	
2	California ISO	David Hawkins		
2	Electric Reliability Council of Texas, Inc.	Roy D. McCoy	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Terry Bilke		
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Affirmative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
3	Alabama Power Company	Robin Hurst	Affirmative	View
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Black Hills Power	Andy Butcher	Affirmative	
3	Blue Ridge Power Agency	Duane S. Dahlquist	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Tallahassee	Rusty S. Foster		
3	Cleco Utility Group	Bryan Y Harper	Affirmative	
3	Cloverland Electric Cooperative	Daniel M Dasho		
3	Commonwealth Edison Co.	Stephen Lesniak		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	Carolyn Ingersoll	Affirmative	
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Douglas County PUD #1	Jeff Johnson		
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	East Kentucky Power Coop.	Sally Witt	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power & Light Co.	W. R. Schoneck	Abstain	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	View
3	Georgia System Operations Corporation	Edward W Pourciau	Negative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Affirmative	View
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	Idaho Power Company	Shaun Jensen	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	View
3	Kissimmee Utility Authority	Gregory David Woessner	Affirmative	
3	Lakeland Electric	Mace Hunter	Negative	
3	Lincoln Electric System	Bruce Merrill	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Abstain	
3	Manitoba Hydro	Jamie Hall	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	View
3	Mississippi Power	Don Horsley	Affirmative	View
3	Modesto Irrigation District	Jack W Savage		
3	New York Power Authority	Michael Lupo	Abstain	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	North Carolina Municipal Power Agency #1	Denise Roeder	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	View
3	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	PacifiCorp	John Apperson	Affirmative	View
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	

3	Portland General Electric Co.	Jerry Thale	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange		
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson		
3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Southern California Edison Co.	David Schiada	Negative	View
3	Tampa Electric Co.	Ronald L. Donahey		
3	Turlock Irrigation District	Casey Hashimoto	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alabama Municipal Electric Authority	Raymond Phillips	Affirmative	View
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Negative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Gayle Mayo	Affirmative	View
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Negative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	Northern California Power Agency	Fred E. Young		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	David W Osburn	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Negative	View
4	Reedy Creek Improvement District	Doug Wagner	Negative	
4	Sacramento Municipal Utility District	Dilip Mahendra	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Black Hills Corp	George Tatar	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Calpine Corporation	John Brent Hebert	Affirmative	
5	City of Farmington	Clinton J Jacobs		
5	City of Tallahassee	Alan Gale	Affirmative	
5	Cleco Power LLC	Grant Bryant	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Negative	View
5	Constellation Generation Group	Michael F. Gildea	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Covanta Energy	Samuel Cabassa	Negative	View
5	Dairyland Power Coop.	Warren Schaefer	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Robert Smith	Negative	
5	Dynegy	Greg Mason	Negative	View
5	Electric Power Supply Association	Jack R. Cashin		
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	FPL Energy	Benjamin Church	Negative	View
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	JEA	Donald Gilbert	Affirmative	
5	Kansas City Power & Light Co.	Scott Heidtbrink	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	

5	Louisville Gas and Electric Co.	Charlie Martin		
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	Michigan Public Power Agency	James R. Nickel	Affirmative	View
5	Montenay Power Corp.	Cleyton Tewksbury	Affirmative	
5	New York Power Authority	Gerald Mannarino	Abstain	View
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	View
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Oglethorpe Power Corporation	Scott McGough	Affirmative	
5	Ontario Power Generation Inc.	Colin Anderson	Negative	View
5	Orlando Utilities Commission	Richard Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp Energy	David Godfrey	Affirmative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik	Negative	
5	Reliant Energy Services	Thomas J. Bradish	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones	Abstain	
5	Southeastern Power Administration	Douglas Spencer	Abstain	
5	Tampa Electric Co.	Frank L Busot		
5	Tenaska, Inc.	Scott M. Helyer	Negative	View
5	Tennessee Valley Authority	Frank D Cuzzort	Negative	View
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Eugene Water & Electric Board	Daniel Mark Bedbury	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Thomas Saitta	Affirmative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Louisville Gas and Electric Co.	Daryn Barker	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	View
6	PacifiCorp	Gregory D Maxfield	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PP&L, Inc.	Thomas Hyzinski	Affirmative	
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	Reliant Energy Services	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Southern California Edison Co.	Marcus V Lotto	Negative	View
6	Tampa Electric Co.	Heidi Giustiniani	Negative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	Corporate Risk Solutions, Inc.	Philip Sobol		
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Other	Michehl R. Gent	Affirmative	
8	Utility Services LLC	Brian Evans-Mongeon	Negative	View

8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	View
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	View
9	North Carolina Utilities Commission	Kimberly J. Jones	Affirmative	
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	View
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	View
10	Northeast Power Coordinating Council, Inc.	Guy Zito	Affirmative	
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

ISO new england

memo

To: Gerry Adamski, NERC, Vice President and Director of Standards

From: Kathleen Goodman, Senior Operations Compliance Coordinator
Joseph Pereira, Cyber-Security Manager
Matthew F. Goldberg, Director, Reliability & Operations Compliance

Date: April 10, 2009

Subject: ISO New England voting comments on Project 2008-06, Cyber Security Standards

As you are aware, ISO New England (ISO-NE) is committed to maintaining and supporting high-quality, enforceable, mandatory Reliability Standards -- a part of which includes the Cyber Security Standards. We have, however, two fundamental enforceability-related concerns with the currently-posted draft. We believe that these concerns warrant a Negative vote. The Standards at issue are CIP-003, R2 and CIP-006, R1.6**.**

To the extent that NERC could sever these two provisions from its filing of the CIP Standard modifications to the Federal Energy Regulatory Commission ("FERC"), or alternatively, FERC (under 18 C.F.R. §39.5(e)) could disapprove, in part, these two aspects of the CIP Standard modifications, ISO-NE would otherwise vote in the Affirmative for these CIP Standard modifications.

A. CIP-003, Requirement 2

Under the Standards as currently drafted (*see specifically* CIP-002), ISO-NE has a single senior manager responsible for approving annually the list of Critical and Critical Cyber Assets. That list has been developed pursuant to a risk-based methodology adopted by the ISO-NE. Under ISO-NE's current management structure, business units (in this case the Information Services Department) are responsible for identifying Critical Cyber Assets. Other Departments with key responsibilities – such as setting the ISO's budget and capital expenditures (as is the case of the Finance Department) – also play a role in ensuring that the Company can implement needed steps to comply. As explained further below, it is difficult to understand how the newly proposed Requirement 2 of CIP-003 has a reasonable relationship to defining or improving upon a "reliability" or "security" objective.

Requirement 2 of CIP-003 states "Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2." There are numerous problems with this new requirement.

ISO New England Inc.
One Sullivan Road, Holyoke, MA 01040-2841
www.iso-ne.com **T** 413 535 4111 **F** 413 535 4343

1. The Requirement Does Not Appear to be a Reliability Standard.

First, this requirement appears to overstep the authority granted to NERC as the ERO under Section 215 of the Federal Power Act in that it attempts to dictate "how" a responsible entity meets compliance with a reliability/security objective – in this case how the company establishes a management structure to achieve compliance. This requirement sets no actual "reliability" or "cybersecurity" performance requirement, and therefore appears to have no reasonable relationship to NERC's authority to set "reliability standards" as that term is defined under Section 215. "Reliability Standards" are "requirement[s] for the operation of existing bulk-power system facilities, including cyber-security protection." **Attempting to dictate, in this instance, how companies organize their management goes well beyond NERC's authority to establish standards governing the "operation" and "protection" of bulk-power system facilities.**

FERC has previously recognized the distinction between regulating "what" registered entities need to do, as opposed to regulating "how" they achieve those reliability/security objectives, and the need for the ERO to balance these considerations. *See* Order No. 672 at P260. By establishing a Standard that seeks to regulate internal management structure without explaining how such a requirement itself establishes greater security, the proposed modification would not appear to address the need to balancing "what" is being regulated versus "how" it is accomplished. **More generally, the entire enforcement regime helps to ensure that companies are doing what is necessary to implement standards. No specific requirement is needed stating as much.**

2. The Standard Drafting Team Provided No Suitable Rationale as Concerns a Non-Reliability or Security Matter.

Second, even if this matter is argued to be within NERC's authority, the Standard Drafting Team provided no suitable justification explaining its purpose. ISO-NE, and other entities, raised this concern in prior comments, and the Standard Drafting Team ("SDT") simply deferred to generic language in Order No. 706. *See, e.g.*, Order No. 706 at P381 (the "Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve."). *See also* U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004) (Blackout Report), Recommendation 43 (recommending that corporations establish "clear authority" for physical and cyber security, and that this "authority should have the ability **to influence** corporate decision-making and the authority to make physical and cyber security-related decisions.") (emphasis added).[1]

However various parties or regulators might interpret what constitutes suitable "influence", achieving the Commission's intent on ensuring that cyber-security matters are given "prominence" within a Responsible Entity could be accomplished in a variety of ways **other than** drafting new Standard requirements. Such other measures could include the manner in which NERC requires periodic reporting by responsible entities, the frequency with which NERC could conduct audits of responsible entities, etc…. In fact, the whole scheme of establishing a phased-

[1] *See* http://www.ferc.gov/industries/electric/indus-act/blackout/ch7-10.pdf

in approach for the CIP Standards acts as a means of ensuring that NERC and Regional Entities *track* Responsible Entities' progress in meeting the Standards – itself a metric for measuring the "prominence" with which the implementation of Standards is given within a Responsible Entity.

The concept of "authority and implementation" – as drafted by the SDT for inclusion as a mandatory *Standard* – simply does not add much to what the FERC and the Blackout Report has previously observed. However, when drafted as a Standard, the language raises issues of: (a) how the SDT intends this requirement to be interpreted, (b) the ERO's specific intent under Section 215 of the Federal Power Act behind approving a requirement that regulates management structure, and (c) how Regional Entities, NERC or FERC would enforce such language.

More generally, it is well understood that SDT may explore a variety of means to address the FERC's concerns. In this instance, given the authority issues raised by NERC Stakeholders, the SDT should have provided more rationale of its proposal. It is especially important for the SDT to provide a robust rationale for its decisions if it attempts to regulate non-technical matters, because FERC is only obligated to give "due weight" to the "technical expertise" of the ERO when determining when to approve a Standard or Standard modification. *See* 18 C.F.R. § 39.5(c)(1). As importantly, given the fact that ERO determinations of a non-technical nature might have *broader* impacts to how other Standards are developed or modified, understanding the thinking of this particular SDT is necessary to ensuring future standards are drafted appropriately.

3. Ambiguity in the Standard Suggests that NERC Intends Responsible Entities to Assign Too Much Authority with One Individual.

As noted above, while the provision itself attempts to address generally expressed concerns in Order No. 706, it also appears to envision a management structure that could be at odds with generally accepted principles of corporate management.

While the phrase "overall responsibility and authority for leading and managing the entity's implementation of, and adherence to" compliance with standards might be susceptible to multiple interpretations, it could unduly "blur the lines" between key Business Officers (for example, between Information Services and Finance as concerns the language relating to "implementation of" compliance). "Implementation" of these standards may involve decisions regarding authorizing capital expenditures, and these decisions may not be within the authority of any specific business unit/manager. These decisions may involve the functions of a Chief Finance Officer or even a Company's Board of Directors, in which case the "overall responsibility and authority" **cannot** sit with a single individual.

Of course, the SDT may have a different concept in mind when it referred to a single individual having "responsibility" and "authority", but the SDT never gave a fulsome explanation of what it had in mind, and *how it was implementing the issues raised in Order No. 706*. **This vagueness should establish real concerns about how this "standard" will be enforced.**

4. Drafting Creates Potential Confusion with Other Standards.

Finally, even if the provision is a justifiable exercise of NERC's authority, ISO-NE believes this requirement is poorly drafted as it should be contained within, and harmonized with, CIP-002. Under CIP-002, some Registered Entities will find that the CIP-002 through -009

requirements do not apply. Moreover, because CIP-002 refers to "a senior manager" having responsibility for approving the Critical and Critical Cyber Asset list, placing this new provision in CIP-003 simply creates unnecessary confusion in how to apply multiple provisions that relate to the same thing in different standards.

B. CIP-006, Requirement 1.6

Requirement 1.6 of CIP-006 states "Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access." Of course, under the current version of the Standard, ISO-NE provides "escorted access" through a variety of means, such as through providing physical escorts and through installing electronic surveillance at access points. Because of the ambiguity regarding "continuous," ISO-NE believes additional information is needed that would support the enforceability/measurement of compliance with the Standard and what is actually needed to implement further measures to ensure compliance. This is particularly important to ISO-NE, because it needs to present its budgeted capital expenditures to its stakeholders for review and advice.

First, with regard to the enforceability, ISO-NE is concerned that "*continuous"* escorted access will prove to be a difficult, if not impossible, Requirement with which registered entities can effectively demonstrate compliance, because of the difficulty determining what records/data can show that such escorting was "uninterrupted."

Second, further information is needed about what "continuous" means, because of the need to develop an appropriate implementation plan to carry out such a requirement. For example, if a company has multiple visitors on site, then the measures employed to ensure "continuous" escorting for each visitor can rapidly increase. For example, if there are multiple personnel working within the Physical Security Perimeter, each one would appear to need a separate escort.

While ISO-NE believes that the concerns raised above warrant continued work on **this requirement** before it should be approved, ISO-NE requests, in the alternative, additional guidance/clarification on how to interpret what constitutes a "continuous" escort.

C. Conclusion

As stated above, ISO-NE takes its CIP Standard compliance very seriously and supports the development of improved CIP Standards. ISO-NE believes that the Standards proposed for approval here, if omitting the Requirements identified above, would themselves establish a more robust CIP Standard regime.

The concerns identified with only these two requirements above were made during the comment period of the drafts now being balloted. In ISO-NE's view, these concerns have not been sufficiently dealt with by the SDT to produce an enforceable, auditable product. A more robust explanation from the SDT might have served to address ISO-NE's concerns, but lacking that, ISO-NE is compelled to raise its objections again at this time. We look forward to working closely with the SDTs in the future to ensure high-quality Standards for protecting the bulk-power system's reliability and cyber-security and enabling robust enforcement.

cc: Jamshid Afnan
Vamsi Chadalavada
Bob Ludlow
Gordon van Welie

ISO New England Inc.
One Sullivan Road, Holyoke, MA 01040-2841
www.iso-ne.com **T** 413 535 4111 **F** 413 535 4343

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on Initial Ballot of CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Summary Consideration:
Most (91.90%) of those who joined the ballot pool to participate in the balloting of the initial set of revisions to the CIP-002-2 through CIP-009-2 standards returned a ballot, and the initial ballot achieved a weighted affirmative vote of 84.06%. There were only 24 negative ballots submitted with a comment, and as can be seen on the following pages, several of these negative comments were submitted by multiple balloters from a single entity registered in multiple industry segments. There were also several comments submitted with affirmative ballots, primarily to provide the SDT with guidance on issues to address in the next phases of revisions to these standards. The major issues raised with affirmative and negative comments include the following:

1) Designation of a single Senior Manager, as required by CIP-003 Requirement R2, is considered to be overly prescriptive and cannot be supported by either the FERC Order 706 or previous SDT responses to similar industry review comments. Entities object to the standards prescribing their corporate governance. To a lesser extent, some entities would prefer to see the Senior Management requirement moved to CIP-002.

In response, the SDT believes the directive in the FERC order appropriately justifies the revision to the existing requirement. The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals.

As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To have attempted to make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comments prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT plans to revisit the placement of the requirement in a future revision to the standards.

2) Entities objected to the addition of "continuous" to CIP-006, Requirement R1.6 with respect to escorted access. Greatest concern is the perceived inability to enforce and audit compliance.

In response, the SDT believes the term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. In response to concerns raised regarding how to demonstrate compliance, the SDT offered that there are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).

3) Entities commented that the Technical Feasibility Exception (TFE) process, as the alternative to "Reasonable Business Judgment" language, should not have been moved to the Compliance Monitoring and Evaluation Program (CMEP) in the NERC Rules of Procedure. Concerns include the need to define the TFE process in the standards themselves and the TFE stipulation that the standard must provide for feasibility or the TFE process will not allow the entity to seek relief. Concerns were also raised with the removal of the assertion in Section D 1.4.2 (Additional Compliance Information) that duly authorized exceptions would not result in non-compliance.

In response, the CIP SDT has no authority over the approval process for changes to the NERC Rules of Procedure, noting the industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees and will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT also believes an exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard and the SDT cannot assert that a properly approved exception to the Responsible Entity's security policy will not result in non-compliance. The exception taken against a company policy is a separate issue from an exception against the requirement of the standard. A Responsible Entity may find it has to process both types of exceptions.

4) A number of modifications were made to the documentation update timeframe requirements, shortening the time from 90 to 30 days. Entities objected to the 30-day timeframe, commenting that the required 30-day timeframe is unrealistic to adequately document and communicate the related changes to all appropriate staff across a company.

In response, the SDT reduced the timeframe for certain documentation requirements to 30 days to conform to applicable directives in the FERC Order 706. For consistency throughout the standards, the SDT reduced the documentation update timeframe to 30 days for the remaining standards requirements that were not directly referenced in the FERC order. The SDT also clarified that the 30-day timeframe begins with the completion of the related change. The SDT believes the 30-day timeframe for updating documentation is appropriate and reasonable.

Version 2 of the CIP Cyber Security Standards (CIP-002 to CIP-009) includes the time-specific directives taken from FERC Order 706 which made a phased implementation approach to revising the standards necessary. The SDT has attempted to provide efficient and effective language to be compliant with the FERC directives while minimizing the impact on the first round of changes.

A number of comments against requirements that were not revised in Version 2 of the standards were deferred with a recommendation to resubmit the comment against Version 3 of the standard if still appropriate.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Voter	Entity	Segment	Vote	Comment
Samuel Cabassa	Covanta Energy	5	Negative	It is not prudent to have the Senior Manager alone do all annual approvals.
Response	The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals.			
Wayne Guttormson	SaskPower	1	Negative	1) Saskatchewan will not adopt these standards as written. We have some serious concerns/questions about the process and end product. First, changes are being mandated by FERC not by Saskatchewan or other Canadian jurisdictions. 2) Secondly, we question the prescriptive nature of most the CIP standards and the philosophy behind them. For example in CIP 002 responses to comments the SDT states that a senior manager is required to be held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. We do not find this argument to be convincing. If this really is the case why do we not use this approach on all of the other standards? Are not the IRO, TOP or EOP stndards just as important as the CIP standards? Shouldn't they be given the prominence they deserve?
Response	1) The SDT understands the concerns regarding a US Government Agency attempting to impose standards upon non-jurisdictional Canadian entities. It may be impractical to have differing requirements for protecting the interconnected Bulk Electric System assets. 2) The requirement for appointing a Senior Manager (CIP-003, Requirement R2) is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT is aware of issues in the existing standards and is working hard to eliminate unnecessary prescription as the standards continue to be revised.			
James R. Nickel	Michigan Public Power Agency	5	Affirmative	MPPA respectfully requests that in the next phase of this project, CIP-003-2 R2 be relocated and inserted as the first requirement of the CIP-002-2 Standard. This is a simple, seemingly non-controversial change which establishes a logical sequence of events and meets FERC's desire for clarity in the NERC process.
Response	As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.			

Voter	Entity	Segment	Vote	Comment
Gayle Mayo	Indiana Municipal Power Agency	4	Affirmative	Indiana Municipal Power Agency (IMPA) is voting affirmative on the CIP standards. In phase II of these standards, IMPA believes that CIP-003 R2 should be moved into CIP-002 R4 in order to clarify the reference to the senior manager. The stakeholders seem to support this improvement, and it should be a relativley simple task or goal for the Standard Drafting Team to perform during phase II.
Response	As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To have attempted to make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.			
William SeDoris Michael K Wilkerson Joseph O'Brien	Northern Indiana Public Service Co. Northern Indiana Public Service Co. Northern Indiana Public Service Co.	3 5 6	Affirmative Affirmative Affirmative	Responses to Comments are inconsistent: 1) Some of the SDT responses to comments provided more clarity than the language drafted within the standard. We believe the same level of clarity should be added to the standard to remove the need for entity interpretation whenever possible. 2) An example of this can be seen in the response to the entities asking for clarification on audit data retention periods. The standard formerly held a three year retention period and in the drafting process the SDT removed this retention limit language. Numerous entities questioned the limit on record retention and the SDT responded that audit records would need to be retained until the completion of the next audit. This additional clarifying language should be added to the standard. 3) Some of the SDT responses to comments provided additional language and interpretations of the modifications made that appear to be unclear in the standards. An example of this is the liability of the CIP designated Senior Manager. It appears that the intent of removing some of the language in the standard regarding entity responsibility was done to clean up the standard and remove redundancy; however some entities questioned if the SDT was placing the responsibility for compliance on the CIP Senior Manager. It is our understanding that the entity is ultimately responsible for compliance with the NERC CIP standard (as is the case with all NERC standards) and the intent of the CIP senior manager designation was for the purpose of a clearly defined individual with responsibility and authority within the entity. The language in the standard supports our belief; however the response to commenters from the SDT seems to go beyond the language in the standard in stating that the Senior Manager is responsible for compliance. If this is the intent of the SDT then the additional language needs to be included within the standard in order to allow for open comments to those modifications.

Voter	Entity	Segment	Vote	Comment
				4) The drafting process All changes and modifications made by the SDT were not clearly identified in the red-lined version that was released for comment. This needs to be prevented from occurring in the future and if identified it needs to be corrected, not accepted and ignored. It may also be considered misleading to an entity to open the latest version of the redlined draft document and only see the modifications that were made from one draft version to the next. It is our belief that the latest red-lined document should identify the modifications made from the original version not just the modifications from the previous draft document. 5) Additionally, comments were submitted in regards to the SDT following the ANSI process that all NERC standards are designed around. It is our belief that the ANSI process should also apply to the standards drafting process and any modifications to the ANSI approved standards format. As the SDT proceeds through the FERC directed changes and modifications are made to the standards, an entity needs to be able to comment on those modifications and receive feedback on the comments submitted. 6) In a number of cases an entity raised a question or a comment on a modification made and the response from the SDT was to defer the question or comment to a later phase. In the NERC standards drafting process when a modification to a standard is proposed, an entity has the ability to comment on the modification when it was proposed. Responses to comments should be provided when the modification was made. If an entity wishes to comment or question language at a later phase the entity would need to file for a clarification. If a change is made through the standards drafting process, and a question or comment is raised by an entity it should not be an acceptable response for the SDT to defer a response to a later phase in the drafting process. 7) The ballot process We would encourage the SDT to treat the CIP standards like all other NERC reliability standards and ballot the standards independent of each other, not as a set of standards. The independent ballot approach would provide for quicker adoption of a standard as it passes ballot. The current approach could result in an entity balloting “No” due to an issue with one standard and as a result they would have no option but to vote “No” to the entire set. If the majority of entities approve of the modifications made to a particular standard, the entities should be allowed to ballot in the modifications made to that standard. The SDT is taking the approach of deferring implementation of a potentially approved standard until the balloting entities approve all modifications to the standards within CIP. This all or nothing approach is counter productive to the rapid adoption and implementation requested by the FERC. If the standards are drafted

Voter	Entity	Segment	Vote	Comment
				independently there would be a great benefit to the entities that are supplying membership to the SDT. As it stands the SDT is tasked with the entire set of modifications and sponsoring entities may not be able to continue that level of support as the process continues. Individual focused drafting teams would limit the scope and impact on a members time and the impact to the sponsoring entity. Approaching the future phases as individual standards will also allow for more targeted subject matter experts to become involved in specific standards as they pertain to their area of expertise.
Response	Thank you for your comments. The SDT offers the following in response to your concerns: 1) To make changes to the language in the standards following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. There were issues that required more substantive debate that the SDT chose to defer to Version 3 of the standards. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. 2) The language in Section D "Compliance" was modified to be consistent with the rest of the NERC standards. 3) The requirement for appointing a Senior Manager (CIP-003, Requirement R2) is to identify a single point of accountability for the implementation and compliance with the CIP standards. 4) As required by the NERC standards development process, there were two red-lined versions available for review. The process requires red-lined revisions since the last posting. "Redline Versions to last approval" are the changes made to the Version 1 standards that were posted for industry comment. "Clean and Redline Versions to last posting" are the incremental changes made to the Version 2 standards in response to the industry comments and are the standards submitted for ballot. 5) The SDT agrees that the ANSI-approved standards drafting process should be followed and believes the process has been followed in this instance. Industry comments were solicited and responses made available prior to the submission to ballot. The Standards Committee approved every step of the process followed. 6) The Version 2 changes to the standards have a very narrow focus, with plans for a more complete revision to follow in future versions. A number of comments were raised against requirements that had not been changed between Version 1 and 2. In this instance, the SDT felt it was appropriate to request the comment be deferred until a future revision of the standards. 7) The CIP standards should be viewed as a complete set, with FERC-mandated, time-specific changes made to all eight Version 2 standards. The SDT believes it is appropriate to ballot the eight version 2 standards as a single set for the Version 2 changes. There is also considerable			

Voter	Entity	Segment	Vote	Comment
	linkage between the eight Version 2 standards, making it very difficult to revise and ballot significant revisions as eight stand-alone standards.			
Ralph Rufrano Michael Lupo Gerald Mannarino	New York Power Authority New York Power Authority New York Power Authority	1 3 5	Abstain Abstain Abstain	1) the phrase " the Senior manager" is deemed to be too prescriptive and 2) the term " continuous escort" may cause compliance issues.
Response	1) The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. Further delegation also needs to be documented to assure the individual granting access or performing other responsibilities normally performed by the Senior Manager has the necessary authorization to do so. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 2) The term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. There are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Alden Briggs	New Brunswick System Operator	2	Negative	1. "Continuous escorted access" is not measurable. How does one prove this? It should be defined. 2. Leadership Role - How an entity is structured to meet compliance to a standard should not be a standard. This could lead to more standards dictating management structure.
Response	1) The term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. There are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control). 2) The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards.			
Larry Akens Frank D	Tennessee Valley Authority Tennessee Valley	1 5	Negative Negative	CIP-006 R1.6 requires a "continuous" escort. This creates a condition that is impossible to prove to auditors. As an alternative, wording might indicate that visitors are to be escorted in a manner to ensure their actions can be supervised and unauthorized disclosures or malicious activities can be prevented, and/or only authorized employees can be escorts.

Voter	Entity	Segment	Vote	Comment
Cuzzort	Authority			
Response	The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Greg Mason	Dynegy	5	Negative	CIP-006, R1.6 requires a "continuos" escort. The word "continuous" creates an unrealistic compliance expectation and one that would be impossible to prove to auditors.
Response	The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Benjamin Church	FPL Energy	5	Negative	CIP 005 R1.6 is not auditable from a compliance stand point. Entities will be unable to sufficiently document compliance with the requirement as written.
Response	The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Kim Warren	Independent Electricity System Operator	2	Affirmative	The IESO votes AFFIRMATIVE so as to move this set of standards forward for further development. However, there still exists a couple of fundamental principle concerns which we expressed earlier, and which we are reiterating below to urge the SDT to address them at the next revision phase a. Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements. Further, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 in CIP-002-2 be revised to: "Annual Approval" The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)" If appointing a senior manager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into

Voter	Entity	Segment	Vote	Comment
				CIP-002 or 2) CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard b. CIP-006 R1.6 should not require "continuous" escorted access. "Continuous" is a condition that is not measurable and hence does not meet the basic characteristics of reliability standards. We suggest this word be removed.
Response	a) The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. Further delegation also needs to be documented to assure the individual granting access or performing other responsibilities normally performed by the Senior Manager has the necessary authorization to do so. As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. b) The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Alan Adamson	New York State Reliability Council	10	Affirmative	The New York State Reliability Council (NYSRC) supports the need to improve the NERC Cyber Security Standards. Despite reservations with certain revisions in this draft version, we believe that overall, the modified standards will improve system reliability. The NYSRC, therefore, has voted in the Affirmative. Because of the following concerns, the NYSRC encourages the Drafting Team to seriously address these issues when the Cyber Security Standards are next modified: 1. CIP-003-1, Requirement 2 - We believe that this requirement, as proposed, oversteps NERC's bounds by giving NERC the authority the dictate corporate governance structure and policy. 2. CIP-006-2, Requirement 1.6 - This requirement does not define what "continuous escorted access" means. Demonstrating compliance with this requirement, as stated, would be very difficult. Removing the word "continuous" would resolve this issue.
Response	1) The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. Further delegation also needs to be documented to assure the individual granting access or performing other responsibilities normally performed by the Senior Manager has the necessary authorization to do so. As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible			

Voter	Entity	Segment	Vote	Comment
	Entities. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 2) The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Kathleen Goodman	ISO New England, Inc.	2	Negative	As you are aware, ISO New England (ISO-NE) is committed to maintaining and supporting high-quality, enforceable, mandatory Reliability Standards -- a part of which includes the Cyber Security Standards. We have, however, two fundamental enforceability-related concerns with the currently-posted draft. We believe that these concerns warrant a Negative vote. The Standards at issue are CIP-003, R2 and CIP-006, R1.6. To the extent that NERC could sever these two provisions from its filing of the CIP Standard modifications to the Federal Energy Regulatory Commission ("FERC"), or alternatively, FERC (under 18 C.F.R. §39.5(e)) could disapprove, in part, these two aspects of the CIP Standard modifications, ISO-NE would otherwise vote in the Affirmative for these CIP Standard modifications. **A. CIP-003, Requirement 2** Under the Standards as currently drafted (*see specifically* CIP-002), ISO-NE has a single senior manager responsible for approving annually the list of Critical and Critical Cyber Assets. That list has been developed pursuant to a risk-based methodology adopted by the ISO-NE. Under ISO-NE's current management structure, business units (in this case the Information Services Department) are responsible for identifying Critical Cyber Assets. Other Departments with key responsibilities – such as setting the ISO's budget and capital expenditures (as is the case of the Finance Department) – also play a role in ensuring that the Company can implement needed steps to comply. As explained further below, it is difficult to understand how the newly proposed Requirement 2 of CIP-003 has a reasonable relationship to defining or improving upon a "reliability" or "security" objective. Requirement 2 of CIP-003 states "Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2." There are numerous problems with this new requirement. **1. The Requirement Does Not Appear to be a Reliability Standard.**

Voter	Entity	Segment	Vote	Comment
				First, this requirement appears to overstep the authority granted to NERC as the ERO under Section 215 of the Federal Power Act in that it attempts to dictate "how" a responsible entity meets compliance with a reliability/security objective – in this case how the company establishes a management structure to achieve compliance. This requirement sets no actual "reliability" or "cybersecurity" performance requirement, and therefore appears to have no reasonable relationship to NERC's authority to set "reliability standards" as that term is defined under Section 215. "Reliability Standards" are "requirement[s] for the operation of existing bulk-power system facilities, including cyber-security protection." **Attempting to dictate, in this instance, how companies organize their management goes well beyond NERC's authority to establish standards governing the "operation" and "protection" of bulk-power system facilities.** FERC has previously recognized the distinction between regulating "what" registered entities need to do, as opposed to regulating "how" they achieve those reliability/security objectives, and the need for the ERO to balance these considerations. *See* Order No. 672 at P260. By establishing a Standard that seeks to regulate internal management structure without explaining how such a requirement itself establishes greater security, the proposed modification would not appear to address the need to balancing "what" is being regulated versus "how" it is accomplished. **More generally, the entire enforcement regime helps to ensure that companies are doing what is necessary to implement standards. No specific requirement is needed stating as much.** **2. <u>The Standard Drafting Team Provided No Suitable Rationale as Concerns a Non-Reliability or Security Matter.</u>** Second, even if this matter is argued to be within NERC's authority, the Standard Drafting Team provided no suitable justification explaining its purpose. ISO-NE, and other entities, raised this concern in prior comments, and the Standard Drafting Team ("SDT") simply deferred to generic language in Order No. 706. *See, e.g.*, Order No. 706 at P381 (the "Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve."). *See also* <u>U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations</u> (April 2004) (Blackout Report), Recommendation 43 (recommending that corporations establish "clear authority" for

Voter	Entity	Segment	Vote	Comment
				physical and cyber security, and that this "authority should have the ability **to influence** corporate decision-making and the authority to make physical and cyber security-related decisions.") (emphasis added).[2] However various parties or regulators might interpret what constitutes suitable "influence", achieving the Commission's intent on ensuring that cyber-security matters are given "prominence" within a Responsible Entity could be accomplished in a variety of ways **other than** drafting new Standard requirements. Such other measures could include the manner in which NERC requires periodic reporting by responsible entities, the frequency with which NERC could conduct audits of responsible entities, etc.... In fact, the whole scheme of establishing a phased-in approach for the CIP Standards acts as a means of ensuring that NERC and Regional Entities *track* Responsible Entities' progress in meeting the Standards – itself a metric for measuring the "prominence" with which the implementation of Standards is given within a Responsible Entity. The concept of "authority and implementation" – as drafted by the SDT for inclusion as a mandatory *Standard* – simply does not add much to what the FERC and the Blackout Report has previously observed. However, when drafted as a Standard, the language raises issues of: (a) how the SDT intends this requirement to be interpreted, (b) the ERO's specific intent under Section 215 of the Federal Power Act behind approving a requirement that regulates management structure, and (c) how Regional Entities, NERC or FERC would enforce such language. More generally, it is well understood that SDT may explore a variety of means to address the FERC's concerns. In this instance, given the authority issues raised by NERC Stakeholders, the SDT should have provided more rationale of its proposal. It is especially important for the SDT to provide a robust rationale for its decisions if it attempts to regulate non-technical matters, because FERC is only obligated to give "due weight" to the "technical expertise" of the ERO when determining when to approve a Standard or Standard modification. *See* 18 C.F.R. § 39.5(c)(1). As importantly, given the fact that ERO determinations of a non-technical nature might have *broader* impacts to how other Standards are developed or modified, understanding the thinking of this particular SDT is necessary to ensuring future standards are drafted appropriately.

[2] *See* http://www.ferc.gov/industries/electric/indus-act/blackout/ch7-10.pdf

Voter	Entity	Segment	Vote	Comment
				3. <u>Ambiguity in the Standard Suggests that NERC Intends Responsible Entities to Assign Too Much Authority with One Individual.</u> As noted above, while the provision itself attempts to address generally expressed concerns in Order No. 706, it also appears to envision a management structure that could be at odds with generally accepted principles of corporate management. While the phrase "overall responsibility and authority for leading and managing the entity's implementation of, and adherence to" compliance with standards might be susceptible to multiple interpretations, it could unduly "blur the lines" between key Business Officers (for example, between Information Services and Finance as concerns the language relating to "implementation of" compliance). "Implementation" of these standards may involve decisions regarding authorizing capital expenditures, and these decisions may not be within the authority of any specific business unit/manager. These decisions may involve the functions of a Chief Finance Officer or even a Company's Board of Directors, in which case the "overall responsibility and authority" **cannot** sit with a single individual. Of course, the SDT may have a different concept in mind when it referred to a single individual having "responsibility" and "authority", but the SDT never gave a fulsome explanation of what it had in mind, and *how it was implementing the issues raised in Order No. 706*. **This vagueness should establish real concerns about how this "standard" will be enforced.** **4. <u>Drafting Creates Potential Confusion with Other Standards.</u>** Finally, even if the provision is a justifiable exercise of NERC's authority, ISO-NE believes this requirement is poorly drafted as it should be contained within, and harmonized with, CIP-002. Under CIP-002, some Registered Entities will find that the CIP-002 through -009 requirements do not apply. Moreover, because CIP-002 refers to "a senior manager" having responsibility for approving the Critical and Critical Cyber Asset list, placing this new provision in CIP-003 simply creates unnecessary confusion in how to apply multiple provisions that relate to the same thing in different standards. **B. <u>CIP-006, Requirement 1.6</u>** Requirement 1.6 of CIP-006 states "Continuous escorted access within the Physical Security

Voter	Entity	Segment	Vote	Comment
				Perimeter of personnel not authorized for unescorted access." Of course, under the current version of the Standard, ISO-NE provides "escorted access" through a variety of means, such as through providing physical escorts and through installing electronic surveillance at access points. Because of the ambiguity regarding "continuous," ISO-NE believes additional information is needed that would support the enforceability/measurement of compliance with the Standard and what is actually needed to implement further measures to ensure compliance. This is particularly important to ISO-NE, because it needs to present its budgeted capital expenditures to its stakeholders for review and advice. First, with regard to the enforceability, ISO-NE is concerned that "*continuous"* escorted access will prove to be a difficult, if not impossible, Requirement with which registered entities can effectively demonstrate compliance, because of the difficulty determining what records/data can show that such escorting was "uninterrupted." Second, further information is needed about what "continuous" means, because of the need to develop an appropriate implementation plan to carry out such a requirement. For example, if a company has multiple visitors on site, then the measures employed to ensure "continuous" escorting for each visitor can rapidly increase. For example, if there are multiple personnel working within the Physical Security Perimeter, each one would appear to need a separate escort. While ISO-NE believes that the concerns raised above warrant continued work on **this requirement** before it should be approved, ISO-NE requests, in the alternative, additional guidance/clarification on how to interpret what constitutes a "continuous" escort. **C. Conclusion** As stated above, ISO-NE takes its CIP Standard compliance very seriously and supports the development of improved CIP Standards. ISO-NE believes that the Standards proposed for approval here, if omitting the Requirements identified above, would themselves establish a more robust CIP Standard regime. The concerns identified with only these two requirements above were made during the comment period of the drafts now being balloted. In ISO-NE's view, these concerns have not been sufficiently dealt with by the SDT to produce an enforceable, auditable product. A more robust explanation from the SDT might have served to address ISO-NE's concerns, but lacking that, ISO-NE is compelled to raise its objections again at this time. We look forward to working closely with the SDTs in the future to ensure high-quality Standards for protecting

Voter	Entity	Segment	Vote	Comment
				the bulk-power system's reliability and cyber-security and enabling robust enforcement.
Response	A) ISO New England expressed concern that CIP-003, Requirement R2 does not appear to be a reliability standard and the SDT provided no suitable rationale as concerns a non-reliability or security matter. ISO-NE also expressed concern that ambiguity in the standard suggests that NERC intends Responsible Entities to assign too much authority with one individual and that this requirement is poorly crafted and creates potential confusion with other standards. The FERC, at Paragraph 381 of Order 706, "requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The Commission agrees with commenters that the senior manager, by virtue of his or her position, is not a user, owner or operator of the Bulk-Power System that is personally subject to civil penalties pursuant to section 215 of FPA." The SDT believes the directive in the FERC order appropriately justifies the revision to the existing requirement. The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals. B) ISO-NE expressed concern that the requirement for "continuous" escort will be difficult to prove to auditors and that additional information is required defining the meaning of "continuous." The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Brian Evans-Mongeon	Utility Services LLC	8	Negative	Utility Services LLC supports the comments as filed by ISO New England regarding this matter. In particular, the "continuous" monitoring aspect is extremely burdensome for smaller entities.
Response	A) ISO New England expressed concern that CIP-003, Requirement R2 does not appear to be a reliability standard and the SDT provided no suitable rationale as concerns a non-reliability or security matter. ISO-NE also expressed concern that ambiguity in the standard suggests that NERC intends Responsible Entities to assign too much authority with one individual and that this requirement is poorly crafted and creates potential confusion with other standards. The FERC, at Paragraph 381 of Order 706, "requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The Commission agrees with commenters that the senior manager, by virtue of his or her position, is not a user, owner or operator of the Bulk-Power System that is personally subject to civil penalties pursuant to section 215 of FPA." The SDT believes the directive in the FERC order appropriately justifies the revision to the existing			

Voter	Entity	Segment	Vote	Comment
	requirement. The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals. B) ISO-NE expressed concern that the requirement for "continuous" escort will be difficult to prove to auditors and that additional information is required defining the meaning of "continuous." The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Gregory Campoli	New York Independent System Operator	2	Affirmative	The NYISO supports continued developement of CIP standards to more affectively address growing security concerns in the industry. The NYISO would also like to identify some issues observed that need to be addressed. CIP-006 Req 1.6 requires continuous escort. It is not clear at this time how this requirement would be monitored or how an entity would show compliance. A requirement should be structured so that compliance is measurable and enforceable.
Response	The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Kent Saathoff	Electric Reliability Council of Texas, Inc.	10	Affirmative	1) Voting affirmative or negative to NERC standards CIP002-2 through CIP009-2 in totality creates a situation where the wording contained in one standard can result in the rejection of solid requirements within other standards. The collective voting of the CIP standards is in direct conflict with the balloting processes used for other NERC Reliability standards. Each standard should be drafted to stand on its own merits and must not hold modifications to any other standard hostage to the weaknesses of a subset. Below are ERCOT's comments regarding the changes proposed to the CIP standards. 2) CIP-002-2 R4 The concept of "the senior manager" is not addressed until CIP-003. It would be advised to clarify who is being referred to here or move the Leadership requirement within CIP-003-2 into CIP-002-2. 3) CIP-003-2 R3 It is unclear as to whether NERC's intent is that the practice under exception cannot commence until an exception is approved. There will be situations where systems, processes, or practices are already well established and in full operation prior to the effective

Voter	Entity	Segment	Vote	Comment
				date of the standards. Clarification of this is requested. 4) CIP-006-2 R1.6 requires a "continuous" escort. Absolutes such as “continuous”, “always”, etc. create a condition that is impossible to prove to auditors and, in most cases, impossible to achieve.
Response	1) The CIP standards should be viewed as a complete set, with FERC-mandated changes made to all eight version 2 standards. The SDT believes it is appropriate to ballot the eight version 2 standards as a single set for the Version 2 changes. 2) As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. The SDT agrees after receiving the industry review comments that the assignment of the Senior Manager would be less confusing if it were moved to CIP-002. However, to make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 3) CIP-003, Requirement R3 provides for the Responsible Entity taking an exception to its Cyber Security Policy required by CIP-003, Requirement R1. This is separate from the proposed modifications to the NERC Rules of Procedure providing for Technical Feasibility Exceptions. Both require compensating measures and those measures can be implemented prior to receiving approval of the applicable exception. 4) The term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. There are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Horace Stephen Williamson Robin Hurst Leslie Sibert Gwen S Frazier Don Horsley	Southern Company Services, Inc. Alabama Power Company Georgia Power Company Gulf Power Company Mississippi Power	1 3 3 3 3	Affirmative Affirmative Affirmative Affirmative Affirmative	1. We are concerned that NERC staff has taken the Technical Feasibility Exception (TFE) process out of the hands of the Standards Drafting Team (SDT) and placed it in the decision making process of NERC staff alone. This will not allow an industry vote on these new Rules of Procedure. 2. This new TFE document, that is out for comments through April 30th, only allow exceptions to be requested for 8 requirements in 2 (of the 8) CIP standards. Entities should be allowed to seek exceptions on all of the CIP requirements if legacy systems prevent them from complying with these current standards. Therefore, we request the SDT initiate that change in Version 3. 3. CIP-006 R1.6 requires a "continuous" escort. This creates a condition that is difficult, if not impossible, to prove to auditors. We suggest that the drafting team work on alternate language to allow for 'supervised' access.

Voter	Entity	Segment	Vote	Comment
Response	1) Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. 2) The suggestion to modify Version 3 of the standards to allow a TFE to be requested for any CIP standard requirement will be considered by the SDT. In the mean time, the SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process. 3) The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).			
Richard J. Kafka	Potomac Electric Power Co.	1	Affirmative	1) Pepco ,indeed all Pepco Holdings affiliates, is concerned about the process used to remove the technical feasibility language and proposed changes to the Rules of Procedure. The industry has been following an implementation schedule for the version 1 set of CIP -002 through CIP-009 for nearly 3 years and are already in or nearing the compliance date and the period to begin documenting compliance. While we understand the need to make the change, there is no discussion of a phase-in of this change. One can anticipate NERC being overwhelmed with TFE Requests and a large number still pending (or even sent back with required changes) after the compliance period for CIP-002 - CIP-009 has begun. The Implementation Plan realistically provides an example showing the effective date as early as January 1, 2010, possibly delayed until April 1 depending on the timing of the approvals. This may force registered entities into non-compliance even though they have been rigorously pursuing compliance. 2) Entities may also be forced into non-compliance if there is no timely response from NERC to the TFE Requests.
Response	1) The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions. The drafting team believes the six to nine month implementation plan is reasonable. 2) Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.			

Voter	Entity	Segment	Vote	Comment
Michael Gammon Charles Locke Thomas Saitta	Kansas City Power & Light Co. Kansas City Power & Light Co. Kansas City Power & Light Co.	1 3 5	Affirmative Affirmative Affirmative	The scope of the Technical Feasibility Exception process should not be limited to the specific CIP requirements listed. It is unrealistic to expect that standard writers will be able to identify in advance all areas that may require a TFE.
Response	Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process.			
Scott M. Helyer	Tenaska, Inc.	5	Negative	Various CIP standards are not acceptable as written without Technical Feasible Exemptions (TFE) being included in the standards themselves or without some reference to TFE approved in another process. As the potential approval of TFE through a separate process is not occurring prior to this vote, then the following CIP standards need to include TFE as follows: CIP-005 R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible. R2.6. Appropriate Use Banner â€" Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible. R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days. CIP-007 R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: R5.3.1. Each password shall be a minimum of six characters. R5.3.2. Each password shall consist of a combination of alpha, numeric, and “special” characters. R5.3.3. Each password shall be changed at least

Voter	Entity	Segment	Vote	Comment
				annually, or more frequently based on risk. R6. Security Status Monitoring" The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP- 008-2.
Response	The proposed TFE process currently allows for TFE Requests against requirements R2.4, R2.6, R3.1 and R3.2 of CIP-005-1, and R2.3, R4, R5.3, R6 and R6.3 of CIP-007-1, and any subsequent versions of these Requirements that continue to expressly provide either (i) that compliance with their terms is required where or as technically feasible or (ii) that technical limitations may preclude compliance with the terms of the Requirement. Per the language in the proposed TFE process, the TFE Request is allowed for the same requirements in version 2 of the CIP standards. Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process.			
Edward W Pourciau Guy Andrews	Georgia System Operations Corporation Georgia System Operations Corporation	3 4	Negative Negative	1) After thorough review of the Proposed Procedure for Requesting and Receiving Technical Feasibility Exception it has became obvious that the CIP Standards CIP-002 through CIP-009 do not account for other possible exceptions to the standards. In addition, there are some inconsistencies in where "technically feasible" and "technical limitation" verbiage is placed within CIP standard or sub-standard. In CIP-007 R5.2.1 the verbiage states "where possibility" and not "technically feasible" 2) In CIP-003 through CIP-009 section D. 1.5 needs to reinstate the statement "Duly authorized exceptions will not result in non-compliance". 3) The "Effective Date" verbiage in all CIP standards is awkward and could be confusing. 4) Recommend verbiage changes for the following sections in all CIP standards: D. Compliance 1.1.2 ERO for Regional Entity and Responsible Entity in certain cases 1.1.3 Third-Party monitor for NERC without vested interest in the outcome. 1.4.1 ..... as part of a Compliance Violation investigation. 1.4.2 term "audit records" is unclear 5) In CIP-003 R5.1 word "logical" should be changed to "Cyber" 6) In CIP-006 R1.8 should read "Review the physical security plan at least once every 12

Voter	Entity	Segment	Vote	Comment
				months" 7) In CIP-007 B. Requirements the verbiage that was deleted in the first line should be reinstated. 8) In CIP-007 R9 and CIP-009 R3 "thirty" should be changed to "sixty"
Response	1) Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. 2) The language in Section D "Compliance" was modified to be consistent with the rest of the NERC standards. 3) A clarifying example of the effective date was included in the "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2" document. 4) The language in Section D "Compliance" was modified to be consistent with the rest of the NERC standards and is defined in the NERC Compliance Monitoring and Evaluation Program (CMEP). The SDT is not able to modify the language as suggested. 5) Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 6) Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 7) The stricken language was duplicative of language in Section A.3., "Purpose." The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 8) The Commission stated in Paragraph 651 of FERC Order 706 that 30 days were sufficient to update the documentation required by CIP-007, Requirement R9. Likewise, the Commission stated in Paragraph 731 of Order 706 that 30 days were sufficient to update the Recovery Plans.			
Dana Cabbell	Southern California Edison Co. Southern California	1 3	Negative Negative	SCE supports the changes in the revised Critical Infrastructure Protection Standards ("CIP Standards"), and greatly appreciates the expedited effort put forth by the 706 Standards Drafting Team ("SDT") to revise the standards. However, SCE is concerned about inconsistencies between the Version 2 CIP Standards, and the NERC's proposed revision to

Voter	Entity	Segment	Vote	Comment
David Schiada Marcus V Lotto	Edison Co. Southern California Edison Co.	6	Negative	the Procedure For Requesting And Receiving Technical Feasibility Exceptions To NERC Critical Infrastructure Protection Standards ("Rules of Procedure"). While SCE understands that the proposed change to the Rules of Procedure is not directly associated with the CIP Version 2 ballot, SCE is of the opinion that the two documents are inextricably linked and cannot be considered independently. SCE's concerns are as follows: 1.) The proposed change to the Rules of Procedure implies that a claim of technical limitation or feasibility represents non-compliance with a requirement. As written, in both Version 1 and 2, there is no language in the requirements that indicate a claim of technical feasibility or limitation, does not meet the requirement. 2.) The revised standards state the following assignment for the SDT CSO706: "…assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure…" SCE is concerned that the proposed revision to the Rules of Procedure was released subsequent to the posting of Version 2 standards revision. Since the revised Rules of Procedure were written after the drafting of the Version 2 standards, the drafting team could not draft to ensure conformance with the Rules of Procedure., rather the team considered the previous version of the Rules of Procedure. SCE does not believe the Version 2 CIP Standards adequately address technical feasibility, and that modifications of the technical feasibility requirements should be handled through modification of the standards themselves, not through a procedural change of the Rules of Procedure. Changing the requirements for the technical feasibility exception through the standards development process will provide clarity to the standards and ensure consistency across the industry. To remedy these concerns, SCE recommends that NERC revise the proposed Rules of Procedure to reflect that the modifications regarding technical limitations or feasibility be applicable to the CIP Version 3 standards under development to ensure clear alignment of the rules of procedure and the CIP standards. This would allow the Version 3 standards to have clear language about the requirements for technical limitations or feasibility. Alternatively, SCE supports an expedited revision to the Version 2 CIP standards intended to clarify the scope and context of technical feasibility limitations within the requirements themselves.
Response	1) An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard. The ERO (NERC) has determined that inability to strictly comply with the requirements of a CIP standard is, in fact, a violation of the standard requirement and has proposed a TFE process whereby the Responsible Entity can remedy the issue without being subject to a finding of violation or imposition of penalties.			

Voter	Entity	Segment	Vote	Comment
	2) Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.			
Martin Bauer	U.S. Bureau of Reclamation	5	Negative	1) The level of specificity in the original version of the standard far exceeds any other reliability standard. This departure in practice was accepted by the utilities because along with the incredible detail, there was an allowance for companies to exercise a certain degree of discretion in implementing the standard. The Commission has "…acknowledged the importance of flexibility and discretion in the CIP NOPR." While the Commission has expressed concern that standards need to be explicit in order to be enforceable it has also expressed that "…the CIP Reliability Standards do not simply allow flexibility, they require it." The Commission appears to understand the concern expressed by utilities in the NOPR process; and, while it required elimination of the term "reasonable business judgment", it has also allowed that "…ERO and the participants in the Reliability Standards development process may choose to develop alternative language to replace reasonable business judgment and propose it for Commission approval." While the standards drafting team was working on addressing the "alternative language", NERC has submitted a Technically Feasible Exemption (TFE) procedure for comment. The draft TFE is more restrictive by eliminating "reasonable business judgment" and "acceptance of risk" as a basis for exemptions. The standards drafting team submitted a revised set of standards that did not include any alternative language. It appears that references in the standards to "reasonable business judgment" and "acceptance of risk" were removed in deference to NERC's draft Technically Feasible Exemption (TFE) procedure which provided a mechanism to request and obtain such exemptions. The presence of the two (NERC Draft TFE and revised CIP002-CIP009 standards) are contradictory to the overall construction of the CIP002-CIP009 standards which relied upon the flexibility afforded by reasonable business judgment. Without the flexibility afforded by alternative language, the level of specificity in the CIP002-CIP009 is unacceptable. Either the alternative language is developed to support the high level of specificity or the standards need to be redrafted to confirm to overall approach used in the other reliability standards. A number of the requirements CIP005 R2.4, 2.6, 3.1, 3.2, CIP007 R4, 5.3, 6, and 6.3 asked that something be done where "technically feasible". These requirements appear to indicate the application of judgment of feasibility, however, no guidance is given on what has to be done when it is not "technically feasible" to remain compliant 2) In addition, the Measures for these standards require the entities to make products of each

Voter	Entity	Segment	Vote	Comment
				requirement conceivably available to any requestor. We believe this poses a security issue.
Response	1) The SDT is diligently working to improve the CIP standards through a phased update approach. Version 2 of the standards removed the "reasonable business judgment" and "acceptance of risk" language as directed by the FERC in Order 706. While FERC Order 706 allowed for the development of alternative language, the SDT was not able to draft any suitable alternative that did not suffer the same issues as the language that was removed. The proposed process for requesting and approving Technical Feasibility Exceptions is a viable alternative. The proposed TFE modifications to the NERC Rules of Procedure define the basis for requesting a TFE and the actions that must be performed by the Responsible Entity to defer findings of non-compliance and imposition of penalties while working to achieve strict compliance with the Applicable Standard. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT also recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 2) The NERC Monitoring and Enforcement Process, approved by Federal regulation, requires compliance data to be made available for inspection by the Compliance Enforcement Authority (CEA), subject to the US and Canadian laws and regulations regarding certain classes of protected information. The CEA Eligible Reviewer is obligated to protect such information from unauthorized disclosure. The proposed TFE process and Section 1500 of the NERC Rules of Procedure prescribe how such sensitive information will be protected. NERC continues to work through the process for dealing with this issue.			
Colin Anderson	Ontario Power Generation Inc.	5	Negative	1) OPG has serious reservations with respect to two areas in the suite of CIP standard revisions: 1.) Multiple areas in the revisions in which the requirements for documenting change have been reduced from 90 to 30 days. These revised timeframes are unrealistic. Rushing such changes will likely create more of a reliability issue than the change itself seeks to remedy. OPG cannot support these revisions. â€¢ CIP-006 R1.7 - The requirement to update the physical security plan within 30 days. â€¢ CIP-007 R9 - The requirement for documenting changes to systems or controls within 30 days â€¢ CIP-008 R1.4 - The requirement to update the Cyber Security Incident Response Plan within 30 calendar days of any changes 2.) CIP-006 R3 - This new requirement, not contemplated in FERC's Order 706, is problematic in situations where a third party is used to monitor and administer portions of the program or where personnel are required to provide remote support to components of the ESP under emergency conditions. OPG submits that this revision has been hastily proposed and not fully considered. 3) OPG is also surprised to see only one ballot (where revisions to all standards must be accepted or rejected as a group). Individual ballots would have better facilitated approvals.
Response	1) Respectfully, the SDT believes the 30-day time frame from the completion of the change for updating documentation is appropriate and			

Voter	Entity	Segment	Vote	Comment
	reasonable. Having up-to-date documentation is essential to the management of the Cyber Assets and response to cyber incidents. 2) CIP-006, Requirement R3 clarifies what was always expected by the CIP Standards. The SDT believes the Cyber Assets used to control and/or monitor ESP access will necessarily be internal to the Responsible Entity's protected network. Remote access for the purposes of contract support or emergency access can be managed like any other approved access into the ESP. 3) The CIP standards should be viewed as a complete set, with FERC-mandated changes made to all eight version 2 standards. The SDT believes it is appropriate to ballot the eight version 2 standards as a single set for the Version 2 changes.			
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Negative	1) Do not fully agree with the SDT responses to comments on CIP-006-R1.7, CIP-008-R1.4, CIP-004-R3, and 2) the response for Question #10 relating to "compliant upon commissioning".
Response	1) The SDT interprets this comment as voicing a concern about reducing the timeframe to update documentation to 30 days. Respectfully, while the SDT acknowledges that the FERC Order 706 did not direct the timeframe to be reduced, the SDT believes 30 days from the completion of the change to update the Security Plan (CIP-006, Requirement R1.7) is no less reasonable than any other documentation update requirement. The SDT reduced this requirement to 30 days to be consistent with the rest of the update requirements throughout the CIP standards. With respect to CIP-008, Requirement R1.4, the SDT believes it is essential that up-to-date response plans be available in the event of an incident. The SDT determined 90 days to update response plans after an incident was too long and selected 30 days to be consistent with the rest of the update requirements throughout the CIP standards. The Commission in FERC Order 706, Paragraph 443, directed that "newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency." The Responsible Entity is given the latitude to define emergency circumstances in its Cyber Security Policy required by CIP-003, Requirement R1. 2) The SDT believes a Cyber Asset being installed as part of a planned change, either a new asset or replacing an existing one, should be evaluated for Critical Cyber Asset status as part of the asset implementation and that compliance with the CIP standards should be built in as part of the project. In doing so, the Cyber Asset is expected to be "compliant upon commissioning."			
Richard Salgo	Sierra Pacific Power Co.	1	Affirmative	1) While I am voting "affirmative" on this ballot, I disagree with the change that was made in four of the Standards (CIP-006 R1.7, CIP-007 R9, CIP-008 R1.4, and CIP-009 R3) to reduce the time period for documentation of various changes from the present 90 days to 30 days. This may be achievable in some instances, however, this is felt to be imposing an undue burden on the entities for no tangible benefit to reliability. 2) As well, we believe that CIP-006 is unclear with respect to requirements around relocation of security access control equipment. Does this require the relocation of such equipment within the Secure Perimeter?

Voter	Entity	Segment	Vote	Comment
Response	1) Respectfully, while the SDT acknowledges that the FERC Order 706 did not direct the timeframe to be reduced, the SDT believes 30 days from completion of the change to update the Security Plan (CIP-006, Requirement R1.7) is no less reasonable than any other documentation update requirement. The SDT reduced this requirement to 30 days to be consistent with the rest of the update requirements throughout the CIP standards. In Paragraph 651 of FERC Order 706, the FERC stated that 30 days was reasonable to update documentation (CIP-007, Requirement R9). The SDT agrees with the FERC assertion. With respect to CIP-008, Requirement R1.4, the SDT believes it is essential that up-to-date response plans be available in the event of an incident. The SDT determined 90 days to update response plans after an incident was too long and selected 30 days to be consistent with the rest of the update requirements throughout the CIP standards. In response to the FERC assertion at Paragraph 731 of FERC Order 706 that recovery plans should be updated within 30 days the SDT modified the CIP-009 requirement to require 30 days for updating the Recovery Plan. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 2) Requirement R2 refers to all components of the physical access control system, including the control panels that interface with the entrance sensors/locking mechanisms and the Cyber Assets used to manage/configure the control panels and interact (HMI interface) with the physical access control system. In Requirement R2.1, the SDT chose to use the terminology “protected from unauthorized physical access” in recognition that not all components of the physical access control system can be reasonably placed within the Physical Security Perimeter. The intent of this requirement is that the Cyber Assets that cannot be reasonably placed within the PSP, such as the HMI interface systems that might reside within the Security Department offices or guard station, be properly secured when not in use to prevent unauthorized reconfiguration of access rights. There is no requirement to relocate all security access control equipment within a Physical Security Perimeter so long as the equipment is protected from unauthorized access.			
John J. Blazekovich	Exelon Energy	1	Affirmative	Exelon does not support the 30 day timeframe for updates to the Phase 1 changes in the areas of physical security plan, recovery plan, systems and controls, and updates to the plan for the response to cyber security incidents documentation because it does not provide sufficient time to complete update, review and approval of documentation with leadership. The proposed 30 day timeframe should be increased to 60 days because in Order 706 there are references to other time periods. For example, P 731 covers R3 of CIP-009 and states, “However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." The 30 day timeframe should also not apply to situations where the entity has made 'administration only' changes to the documentation or other changes driven by internal business requests and/or decisions
Response	Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.			
Thomas C. Mielnik	MidAmerican Energy Co.	3	Affirmative	1) MidAmerican is concerned that the following statement has been removed throughout the standards: Duly authorized exceptions will not result in noncompliance. This sentence should be included in CIP-003-2, R3. This retains the clarity in version 1 that authorized exceptions are not violations.

Voter	Entity	Segment	Vote	Comment
				2) Exclude the client side of client-server applications used for access control and/or monitoring from CIP-006-2 protection requirements in R2 and R3.
Response	1) An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard. The proposed modification to the NERC Rules of Procedure regarding Technical Feasibility Exceptions provides the appropriate relief from findings of non-compliance, subject to the terms of the TFE being met. The SDT cannot assert that a properly approved exception to the Responsible Entity's security policy will not result in non-compliance. 2) The client side systems, such as the HMI interface, need to be protected from unauthorized access.			
Charles W. Jenkins	Oncor Electric Delivery	1	Affirmative	Although NERC interpretation 2007-27, requested by SCE&G, is not included in Version 2, we rely on NERC's interpretation specifically stating that dial-up Critical Cyber Assets do not require physical protection required by CIP-006.
Response	Respectfully, neither the NERC BOT nor the FERC has adopted the referenced interpretation.			
Harvie D. Beavers	Colmac Clarion/Piney Creek LP	5	Negative	Changes have taken a fairly confusing set of standards and converted them into a nearly 'all encompassing' lawyers dream. Almost every generation facility has a control system that is a 'routable protocol', yet many have no external control or access, thus are not 'vulnerable' to external attack. Appears that all will have to be available to interpretation of current wording by not only plant managemnet but any audit action. The 'criticality' of a generating asset is proportional to how many are operating in each load section and the load they are supplying. Current Glossary added to these procedures can be inferred to make everything a critical asset
Response	The determination on whether a facility is a Critical Asset is made independent of whether the cyber assets within it are critical cyber assets. This determination for cyber assets only occurs after a facility is declared a Critical Asset: there has been no change made to the glossary from version 1 to version 2. The current standards clearly state that for a cyber asset to be declared critical, it must satisfy the requirements of CIP-002 R3.1, R3.2 or R3.3: in the case of cyber assets which do not satisfy any of these criteria, they are not required to be declared Critical Cyber Assets.			
Thomas J. Szelistowski	Tampa Electric Co.	1	Negative	1) CIP Standards Version 2 comments Implementation Plan Table 1 examples. How would an entity handle the reclassification of an asset from Cyber Asset to Critical Cyber Asset due to a new or re-interpretation of the wording and intent of the standard where the entity's methodology did not necessarily change. 2) P5 Table 2. Depending upon the size and scope of the Critical Asset coming under the standard and entity subject to category 2 compliance will need more than 12 months to come into compliance with the requirements of CIP005 through CIP007. A significant effort is involved in planning for the execution of many of these requirements. Additionally, fiscal planning cycles may not align with the timing of the asset being deemed critical, leaving

Voter	Entity	Segment	Vote	Comment
				considerably less than 12 months for actual application of the standards. A 12 month cycle serves as a dis-incentive to the entity in declaring the asset critical as soon as it is aware of the need for reclassification. We suggest that at a minimum 24 months be allowed. 3) P6 CIP002 through CIP009 General Comments Page numbering inaccurate, making review difficult 4) Throughout, applicability provides exemption to facilities regulated under the US Nuclear Regulatory Commission. Needs to be updated to reflect recent FERC ruling. 5) While the drafting team is performing edits to this document, it might be an appropriate time to remove some of the cross referrals within CIP005 and CIP006 to other standards. These can lead to confusion and mis-interpretation during implementation. Our organization and others within our region have had to create internal matrices to track all of these cross referrals. This draft introduces more cross referrals. If these must remain, then perhaps the drafting team can maintain either as a part of the standards or as a separate document a matrix that the industry can rely upon for consistency. 6) For all revised standards, the Data Retention information 1.3 states Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. The retention use to be three years and the registered entity had no responsibility to maintain audit records. It is not clear for registered entities what “last audit records” includes? Please detail what is considered an “audit record.” In addition, based on current wording, “and all requested and submitted subsequent audit records”, subsequent records (which would mean after the audit) appear to need to be retained forever. 7) We continue to have serious concerns related to the “exception process” as we indicated in our last comments (Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems” and your response (Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. 8) The technical feasibility exception process will address the requirements for documenting,

Voter	Entity	Segment	Vote	Comment
				approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.) As the TFE process is now drafted, it addresses only those areas where technical infeasibility is mentioned in the standard. 9) There are other requirements where it may be operationally unsafe or technically infeasible to meet. Under version 1 standards, this was recognized and provisions made to allow for exceptions without non-compliance. Under this version, it would appear that an exception to our cyber security policy may result in non-compliance. If this is the intent, the drafting team should review every requirement and identify every requirement where operational or technical infeasibility may be applicable so that the TFE process may be followed. 10) CIP002- no comments 11) CIP003 - It is not clear if this standard is going to be modified to incorporate or reflect the Technical Feasibility Exception process that is under development by NERC. We expect that the drafting team is working with NERC to reconcile this standard with the newly proposed process. 12) CIP004 - no comments 13) CIP005 - R1.5 needs clarification. Is the intent to protect devices which do security monitoring or should it include any type of monitoring which is done? Devices which perform performance monitoring of the perimeter, such as bandwidth analysis, etc should not be subject to these requirements as an access control or monitoring device. They may be a cyber asset within the perimeter, but they may be performing their performance monitoring from outside the perimeter. We suggest the following wording change: "Cyber Assets used in the access control and/or security monitoring of the Electronic Security Perimeter...." R1.5 Afforded the protective measures of .....Standard CIP-006-2 Requirement R3 It is not clear how one monitors the physical security perimeter CIP006 -R3 when it is not required to have one around the devices listed in CIP005 R1.5 14) CIP006 - No comment 15) CIP007 - no comments 16) CIP008 - no comments

Voter	Entity	Segment	Vote	Comment
				17) CIP009 - no comments
Response	1) This would be treated the same as an unplanned change due to a change in system conditions. The Responsible Entity would need to document why the new Critical Asset or Critical Cyber Asset is only now being identified. 2) The 12-month timeframe is reasonable for most instances. Both the Self-Report with mitigation plan and the proposed TFE process changes to the NERC Rules of Procedure provide for requesting additional time to comply. 3) Thank you for your comment. The SDT apologizes for the inconvenience and has made NERC staff aware of the issue. 4) The exemption language is consistent with the definition of "facility" in FERC Order 706B at Paragraph 11. FERC clarified its terminology at Paragraphs 14 and 15. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. This is an administrative change that can be accommodated separately. 5) Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 6) The language in Section D "Compliance" was modified to be consistent with the rest of the NERC standards. 7) An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard. The exception taken against a company policy is a separate issue from an exception against the requirement of the standard. A Responsible Entity may find it has to process both types of exceptions. Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. 8) Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. 9) The observation is correct. An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard. Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have			

Voter	Entity	Segment	Vote	Comment
				another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process. 10) Thank you. 11) While the CIP SDT will consider the TFE issue in future revisions to the standards, the proposed TFE process is a separate document under the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. 12) Thank you. 13) The SDT understands this comment to suggest adding the word "security" before "monitoring." Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate. 14) Thank you. 15) Thank you. 16) Thank you. 17) Thank you.
James R. Keller Anthony Jankowski Linda Horn	Wisconsin Electric Power Marketing Wisconsin Energy Corporation Wisconsin Electric Power Company	3 4 5	Negative Negative Negative	1) Comments on CIP 006-2, R2.1 We Energies understands that this requirement refers to the programmable logic controller in a card reader system that is often referred to as the "panel". The panel is the intelligent device that serves a card reader-controlled door. The proposed text requires protection of the panels from unauthorized physical access. We believe that the use of the word "unauthorized" establishes a more stringent requirement than that which the drafting team intended. We believe this because authorization implies establishment of a list of individuals who have been authorized to physically access the asset and implies the installation of some mechanism to distinguish between authorized and unauthorized attempts to physically access the panel door. In effect, it appears to create a duty to add a card reader to the panel door, itself. We Energies agrees that the panels need to be protected against physical tampering and we believe that installation of a key lock and intrusion detection capability for the panel door is appropriate and adequate. Accordingly, we believe that R2.1 should have read, "Be protected from undetected physical access." If this was the drafting

Voter	Entity	Segment	Vote	Comment
				team's intention, We Energies requests this clarification. 2) Comments on CIP 006-2, R2.2 We Energies understands that this requirement refers to the programmable logic controller in a card reader system that is often referred to as the "panel". The panel is the intelligent device that serves a card reader-controlled door. The proposed text appears to require that the panels be protected from physical tampering by placing them inside an already-protected physical security perimeter (PSP), or appears to require construction of a new PSP solely to protect the panel. The former sometimes can be easily accomplished by moving a panel from a location just outside the PSP to a location just inside the PSP. The latter is more challenging when the panel is distant from the PSP, sometimes separated by hundreds of feet and substantial barriers. We Energies agrees that the panels need to be protected against physical tampering and placing them inside a PSP offers better protection than leaving them outside a PSP. Locking the panel door and installing intrusion detection on the door is even better. However, these do not offer protection against cyber tampering. For instance, a panel is not protected against cyber tampering at the point where the panel's data communications cable connects to the LAN/WAN network in a remote data closet. Simply unplugging this cable in the data closet and connecting it to a laptop PC on which has been installed the access control system application affords an individual the ability to tamper with the data and settings in the panel. We Energies can eliminate the risk to the data and settings in the panel without physically moving it by replacing the conventional copper data cable with a fiber-optic cable and encrypting the communications. This is more effective than physically moving the panel to a location inside a PSP. We Energies suggests establishment of an option under R2 which would permit such a technical alternative to physically relocating the panels.
Response	1) Requirement R2 refers to all components of the physical access control system, including the control panels that interface with the entrance sensors/locking mechanisms and the Cyber Assets used to manage/configure the control panels and interact (HMI interface) with the physical access control system. In Requirement R2.1, the SDT chose to use the terminology "protected from unauthorized physical access" in recognition that not all components of the physical access control system can be reasonably placed within the Physical Security Perimeter. The intent of this requirement is that the Cyber Assets that cannot be reasonably placed within the PSP, such as the HMI interface systems that might reside within the Security Department offices or guard station, be properly secured when not in use to prevent unauthorized reconfiguration of access rights. 2) Requirement R2 refers to all components of the physical access control system, including the control panels that interface with the entrance sensors/locking mechanisms and the Cyber Assets used to manage/configure the control panels and interact (HMI interface) with the physical access control system. In Requirement R2.2, placing the panel referred to in the comment within the PSP it controls, or any other suitable PSP, is consistent with SDT's understanding the requirement. Protecting the connecting data cable from unauthorized access via the data closet is also expected if required to prevent unauthorized logical access as described in the comment.			

Voter	Entity	Segment	Vote	Comment
Raymond Phillips	Alabama Municipal Electric Authority	4	Affirmative	I understand why the SDT decided to approach changes to the CIP standards in phases but it makes for a lot of additional work on everyone involved.
Response	Included in the FERC Order 706 were time-specific directives that made a phased implementation approach necessary. The SDT has attempted to minimize the impact of the first round of changes as much as possible.			
Catherine Koch	Puget Sound Energy, Inc.	1	Affirmative	PSE votes affirmative with version 2 changes, but anticipates the opportunity to provide more detailed comment regarding each standard in general when version 3 draft is available for comment. The standards are in need of further clarity to ensure compliance in the most effective manner.
Response	Thank you for your comment. The SDT looks forward to your comments when Version 3 of the standards is submitted for industry review.			
Anita Lee	Alberta Electric System Operator	2	Abstain	The AESO is not certain of the impact of these standards on the market and grid operation in Alberta.
Response	Thank you for your comment. Respectfully, the SDT is not able to respond to your concern.			
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4	Negative	The District understands the removal of “reasonable business judgment” was done in accordance with FERC Order 706 and the proposed Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment. The District agrees that “reasonable business judgment” is not the ideal statement however we are also concerned with the response that the proposed “Technical Feasibility Exception Process should address the concerns”. A more prescriptive process may address this concern but it could just as likely produce unacceptable consequences. The District believes that assessment of risk and engineering/economic judgment are all necessary skills when assessing critical assets. It is important to understand the impacts that a cyber or other failure may have on the Bulk Electric System and assess the risk internally as well as neighboring systems. This assessment must focus on risk/exposure and the level of impact. There are many risks to the electric industry, and it is important that the standards focus limited resources on addressing exposures by include risk levels and impacts into the decision making process.
Response	The Version 2 revisions to the CIP standards are intended to address the time-specific changes mandated by the FERC. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.			
John Apperson David Godfrey	PacifiCorp	3 5	Affirmative Affirmative	The following statement has been removed throughout the standards: "Duly authorized exceptions will not result in noncompliance." While PacifiCorp understands that the proposed NERC procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards is intended to provide guidance and clarity on how these necessary exceptions will be viewed by NERC, the standards as presented lack the clarity that authorized exceptions are not violations.
Response	An exception taken against the Responsible Entity’s compliance policy does not relieve the entity from compliance with the requirement of the			

Voter	Entity	Segment	Vote	Comment
	standard. The proposed modification to the NERC Rules of Procedure regarding Technical Feasibility Exceptions provides the appropriate relief from findings of non-compliance, subject to the terms of the TFE being met. The SDT cannot assert that a properly approved exception to the Responsible Entity's security policy will not result in non-compliance.			
William Mitchell Chamberlain Diane J. Barney	California Energy Commission National Association of Regulatory Utility Commissioners	9 9	Affirmative Affirmative	This affirmative vote is based on the continuing nature of Project 2008-06 which needs to address ambiguous language being identified by parties, and the belief that NERC audit activities will take into account known issue areas yet to be addressed within the Project.
Response	Thank you for your comment. The SDT is already working on additional revisions to the CIP standards. Please be sure to comment on future revisions to the standards when posted for industry review.			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Recirculation Ballot Window Open

April 17–27, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Revisions to Cyber Security Standards CIP-002-1 through CIP-009-1 (Project 2008-06)

A recirculation ballot window for revisions to cyber security standards CIP-002-1 through CIP-009-1 is now open **until 8 p.m. EDT on April 27, 2009.** The posting includes an associated implementation plan for the standards. The page numbers in CIP-002-2 and CIP-003-2 have been corrected.

Project Background

The Cyber Security Standard Drafting Team has been assigned the responsibility of revising the cyber security standards as follows:

- ensure the standards conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure,
- address the directed modifications identified in FERC Order 706, and
- consider other cyber-related standards, guidelines, and activities.

The drafting team subdivided its work into multiple phases, with "Phase I" (the current phase) focused on addressing near term directives in FERC Order 706. The most significant of these revisions addresses the directive to remove references to "reasonable business judgment" before compliance audits begin in 2009. All issues that will require significant industry debate were deferred to later phases of the project to ensure that the FERC imposed deadline for removing "reasonable business judgment" can be met.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Recirculation Ballot Process

The Standards Committee encourages all members of the Ballot Pool to review the consideration of comments submitted with the initial ballots. In the recirculation ballot, votes are counted by exception only — if a Ballot Pool member does not submit a revision to that member's original vote, the vote remains the same as in the first ballot. Members of the ballot pool may:

- Reconsider and change their vote from the first ballot.
- Vote in the second ballot even if they did not vote on the first ballot.
- Take no action if they do not want to change their original vote.

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Final Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Revisions to Cyber Security Standards CIP-002-1 through CIP-009-1 (Project 2008-06)

The ballot pool approved the standards revisions. The revised standards will be submitted to the NERC Board of Trustees for adoption.

The recirculation ballot for revisions to cyber security standards CIP-002-1 through CIP-009-1 ended April 27, 2009. The final ballot results are shown below. The Ballot Results Web page provides a link to the detailed results.

Quorum: 94.37%
Approval: 88.32%

Ballot Criteria

Approval requires both:

- A quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention; and
- A two-thirds majority of the weighted segment votes cast must be affirmative. The number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses.

Project Background

The Cyber Security Standard Drafting Team has been assigned the responsibility of revising the cyber security standards as follows:

- ensure the standards conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure,
- address the directed modifications identified in FERC Order 706, and
- consider other cyber-related standards, guidelines, and activities.

The drafting team subdivided its work into multiple phases, with “Phase I” (the current phase) focused on addressing near term directives in FERC Order 706. The most significant of these revisions addresses the directive to remove references to “reasonable business judgment” before compliance audits begin in 2009. All issues that will require significant industry debate were deferred to later phases of the project to ensure that the FERC imposed deadline for removing “reasonable business judgment” can be met.

Project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Applicability of Standards in Project

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

An associated implementation plan is posted for the standards.

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results

Ballot Name:	Project 2008-06 CIP-002-1-CIP-009-1 Revisions_rc
Ballot Period:	4/17/2009 - 4/27/2009
Ballot Type:	recirculation
Total # Votes:	268
Total Ballot Pool:	284
Quorum:	**94.37 % The Quorum has been reached**
Weighted Segment Vote:	88.32 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	77	1	62	0.886	8	0.114	4	3
2 - Segment 2.	10	0.7	5	0.5	2	0.2	1	2
3 - Segment 3.	67	1	54	0.947	3	0.053	5	5
4 - Segment 4.	23	1	17	0.85	3	0.15	2	1
5 - Segment 5.	59	1	43	0.827	9	0.173	4	3
6 - Segment 6.	30	1	25	0.926	2	0.074	2	1
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	6	0.5	4	0.4	1	0.1	0	1
9 - Segment 9.	4	0.4	4	0.4	0	0	0	0
10 - Segment 10.	8	0.8	8	0.8	0	0	0	0
Totals	**284**	**7.4**	**222**	**6.536**	**28**	**0.864**	**18**	**16**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman		
1	ATCO Electric	Doug Smeall	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	

1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	View
1	CenterPoint Energy	Paul Rocha	Negative	
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Alan L Cooke	Affirmative	
1	City Utilities of Springfield, Missouri	Jeff Knottek	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	E.ON U.S. LLC	Larry Monday	Abstain	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	View
1	Farmington Electric Utility System	Alan Glazner	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	C. Martin Mennes	Abstain	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	JEA	Ted E. Hobson		
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	View
1	Kissimmee Utility Authority	Joe B Watson	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	Rodney Hawkins	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	Minnesota Power, Inc.	Carol Gerou	Affirmative	
1	National Grid	Manuel Couto	Affirmative	
1	Nebraska Public Power District	Richard L. Koch	Affirmative	
1	New Brunswick Power Transmission Corporation	Brian Scott	Affirmative	
1	New York Power Authority	Ralph Rufrano	Affirmative	View
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Oncor Electric Delivery	Charles W. Jenkins	Affirmative	View
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	View
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Puget Sound Energy, Inc.	Catherine Koch	Affirmative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SaskPower	Wayne Guttormson	Negative	View
1	Seattle City Light	Pawel Krupa	Affirmative	View
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	View
1	South Texas Electric Cooperative	Richard McLeon	Affirmative	
1	Southern California Edison Co.	Dana Cabbell	Abstain	View
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Abstain	
1	Tampa Electric Co.	Thomas J. Szelistowski	Negative	View
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Transmission Agency of Northern California	James W. Beck	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	

1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Western Farmers Electric Coop.	Alan Derichsweiler	Affirmative	
1	Xcel Energy, Inc.	Gregory L. Pieper	Affirmative	
2	Alberta Electric System Operator	Anita Lee	Abstain	View
2	British Columbia Transmission Corporation	Phil Park	Affirmative	
2	California ISO	David Hawkins		
2	Electric Reliability Council of Texas, Inc.	Roy D. McCoy	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Terry Bilke		
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Affirmative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
3	Alabama Power Company	Robin Hurst	Affirmative	View
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Black Hills Power	Andy Butcher	Affirmative	
3	Blue Ridge Power Agency	Duane S. Dahlquist	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City of Tallahassee	Rusty S. Foster		
3	Cleco Utility Group	Bryan Y Harper	Affirmative	
3	Cloverland Electric Cooperative	Daniel M Dasho	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	Carolyn Ingersoll	Affirmative	
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Douglas County PUD #1	Jeff Johnson		
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	East Kentucky Power Coop.	Sally Witt	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power & Light Co.	W. R. Schoneck	Abstain	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	View
3	Georgia System Operations Corporation	Edward W Pourciau	Negative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Affirmative	View
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	Idaho Power Company	Shaun Jensen	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	View
3	Kissimmee Utility Authority	Gregory David Woessner	Affirmative	
3	Lakeland Electric	Mace Hunter	Negative	
3	Lincoln Electric System	Bruce Merrill	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Abstain	
3	Manitoba Hydro	Jamie Hall	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	View
3	Mississippi Power	Don Horsley	Affirmative	View
3	Modesto Irrigation District	Jack W Savage		
3	New York Power Authority	Michael Lupo	Abstain	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	North Carolina Municipal Power Agency #1	Denise Roeder	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	View
3	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	PacifiCorp	John Apperson	Affirmative	View
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	

3	Portland General Electric Co.	Jerry Thale	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson		
3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	View
3	Southern California Edison Co.	David Schiada	Abstain	View
3	Tampa Electric Co.	Ronald L. Donahey		
3	Turlock Irrigation District	Casey Hashimoto	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alabama Municipal Electric Authority	Raymond Phillips	Affirmative	View
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Negative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Gayle Mayo	Affirmative	View
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	Northern California Power Agency	Fred E. Young		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	David W Osburn	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Negative	View
4	Reedy Creek Improvement District	Doug Wagner	Negative	
4	Sacramento Municipal Utility District	Dilip Mahendra	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	View
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Calpine Corporation	John Brent Hebert	Affirmative	
5	City of Farmington	Clinton J Jacobs		
5	City of Tallahassee	Alan Gale	Affirmative	
5	Cleco Power LLC	Grant Bryant	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	View
5	Constellation Generation Group	Michael F. Gildea	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Covanta Energy	Samuel Cabassa	Negative	View
5	Dairyland Power Coop.	Warren Schaefer	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Robert Smith	Negative	
5	Dynegy	Greg Mason	Negative	View
5	Electric Power Supply Association	Jack R. Cashin		
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	FPL Energy	Benjamin Church	Negative	View
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	JEA	Donald Gilbert	Affirmative	
5	Kansas City Power & Light Co.	Scott Heidtbrink	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	

5	Louisville Gas and Electric Co.	Charlie Martin	Abstain	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	Michigan Public Power Agency	James R. Nickel	Affirmative	View
5	Montenay Power Corp.	Cleyton Tewksbury	Affirmative	
5	New York Power Authority	Gerald Mannarino	Abstain	View
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	View
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Oglethorpe Power Corporation	Scott McGough	Affirmative	
5	Ontario Power Generation Inc.	Colin Anderson	Negative	View
5	Orlando Utilities Commission	Richard Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp Energy	David Godfrey	Affirmative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik	Negative	
5	Reliant Energy Services	Thomas J. Bradish	Affirmative	
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones	Abstain	
5	Southeastern Power Administration	Douglas Spencer	Abstain	
5	Tampa Electric Co.	Frank L Busot		
5	Tenaska, Inc.	Scott M. Helyer	Negative	View
5	Tennessee Valley Authority	Frank D Cuzzort	Affirmative	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	View
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Eugene Water & Electric Board	Daniel Mark Bedbury	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Thomas Saitta	Affirmative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Louisville Gas and Electric Co.	Daryn Barker	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	View
6	PacifiCorp	Gregory D Maxfield	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PP&L, Inc.	Thomas Hyzinski	Affirmative	
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	Reliant Energy Services	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Southern California Edison Co.	Marcus V Lotto	Abstain	View
6	Tampa Electric Co.	Heidi Giustiniani	Negative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	Corporate Risk Solutions, Inc.	Philip Sobol		
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Other	Michehl R. Gent	Affirmative	
8	Utility Services LLC	Brian Evans-Mongeon	Negative	View

8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	View
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	View
9	North Carolina Utilities Commission	Kimberly J. Jones	Affirmative	
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	View
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	View
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Exhibit C

The Cyber Security Standard Drafting Team Roster

Exhibit C
Cyber Security Order 706 Standard Drafting Team Roster (Project 2008-06)

Jeri Domingo Brewer — Chair Special Assistant	U.S. Bureau of Reclamation 2800 Cottage Way — MP-106 Sacramento, California 95825	(916) 978-5198 jbrewer@mp.usbr.gov
Kevin B. Perry — Vice Chair Director, Critical Infrastructure Protection	Southwest Power Pool Regional Entity 415 North McKinley — Suite 140 Little Rock, Arkansas 72205	(501) 614-3251 (501) 664-6923 Fx kperry@spp.org
Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@opg.com
Jackie Collett Cyber Security Operations Engineer	Manitoba Hydro 1565 Willson Place — P.O. Box 815 Winnipeg, Manitoba R3C 2P4	(204) 477-7709 jcollett@hydro.mb.ca
Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@southernco.com
Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@kcpl.com
Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets — 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@duke-energy.com
Scott W. Fixmer Senior Security Analyst Exelon Corporate Security	Exelon Corporation 1700 Spencer Road Joliet, Louisiana 60433	(815) 724-7203 (815) 724-7032 Fx Scott.Fixmer@exeloncorp.com
Gerald S. Freese Director, Enterprise Information Security	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
Philip Huff Security Analyst	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
Frank Kim Director, Power System Information Technology	Hydro One Networks, Inc. 49 Sarjeant Drive Barrie, Ontario L4N 4V9	(705) 792-3033 frank.kim@hydroone.com
Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
John Lim, CISSP Department Manager	Consolidated Edison Co. of New York 4 Irving Place — Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
David L. Norton Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue — MS: L-ENT-24A New Orleans, Louisiana 70113	(504) 576-5469 (504) 576-5123 Fx dnorto1@entergy.com

Christopher A. Peters Vice President, Cybersecurity Solutions	ICF International 9300 Lee Highway Fairfax, Virginia 22031	(703) 934-3864 cpeters@icfi.com
David S Revill Group Lead, Electronic Maintenance	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@gatrans.com
Scott Rosenberger Manager of Information Technology	Luminant Energy 500 North Akard Dallas, Texas 75201	(214) 875-8731 scott.rosenberger@luminant.com
Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
Jon Stanford Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@bpa.gov
Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive — Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 Fx keith.stouffer@nist.gov
John D. Varnell Technology Director	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 Fx jvarnell@tnsk.com
William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue — Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@aps.com
Hal Beardall — Consultant to NERC	Florida State University Morgan Building — Suite 236 2035 East Paul Dirac Drive — P.O. Box 3062777 Tallahassee, Florida 32310-4161	(850) 644-4945 (850) 644-4968 Fx hbeardall@fsu.edu
Joseph Bucciero President and Executive Consultant — **Consultant to NERC**	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525	(267) 981-5445 joe.bucciero@gmail.com
Robert M. Jones Director Florida Conflict Resolution Consortium — **Consultant to NERC**	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive Tallahassee, Florida 32310-4161	(850) 644-6320 (850) 644-4968 Fx rmjones@fsu.edu
Stuart Langton, PhD Senior Fellow — **Consultant to NERC**	Florida State University 2010 Wild Lime Drive Sanibel, Florida 33957	(239) 395-9694 (239) 395-3230 Fx slangton@mindspring.com
Tom Hofstetter NERC Regional Compliance Auditor	North American Electric Reliability Corporation Noblesville, Indiana 46062	609-651-2532 (609) 452-0550 Fx tom.hofstetter@nerc.net
Roger Lampila NERC Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx roger.lampila@nerc.net
Scott Mix NERC Manager of Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (801) 203-8204 Fx scott.mix@nerc.net

Julia Souder NERC Director of Inter-Governmental Relations	North American Electric Reliability Corporation 1120 G Street, N.W. — Suite 990 Washington, D.C. 20005-3801	(202) 393-3998 (202) 393-3955 Fx julia.souder@nerc.net
David Taylor NERC Manager of Standards Development	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx david.taylor@nerc.net
Todd Thompson NERC Compliance Investigator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx todd.thompson@nerc.net

Exhibit D

CIP Standards Redline/Strikeout Version
Proposed Changes to Standards

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-1~~1~~2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-002-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-002:~~

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — ~~A~~ The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of

the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:~~

M1. ~~The~~ Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. ~~The~~The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 ~~Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor~~None.

2. ~~Levels of Non-Compliance~~Violation Severity Levels (To be developed later.)

~~**2.1 Level 1:** The risk assessment has not been performed annually.~~

~~**2.2 Level 2:** The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.~~

~~**2.3 Level 3:** The list of Critical Assets or Critical Cyber Assets does not exist.~~

~~**2.4 Level 4:** The lists of Critical Assets and Critical Cyber Assets do not exist.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~1~~2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~.~~ ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-003:~~

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, ~~business phone, business address,~~ and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures~~, or a statement accepting risk~~.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or ~~-~~delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, ~~business phone~~ and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements~~ Responsible Entity shall make available documentation of ~~Standard CIP-003:~~

M1. ~~Documentation of the Responsible Entity's~~its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. ~~Documentation~~ The Responsible Entity shall make available documentation of the assignment of, and changes to, ~~the Responsible Entity's~~its leadership as specified in Requirement R2.

M3. ~~Documentation of the Responsible Entity's~~ The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. ~~Documentation of the~~The Responsible ~~Entity's~~Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible ~~Entity's~~Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.~~

~~**2. Levels of Noncompliance**~~

~~**2.1. Level 1:**~~

~~**2.1.1** Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,~~

~~**2.1.2** Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,~~

~~**2.1.3** An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.~~

~~**2.2. Level 2:**~~

~~**2.2.1** A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,~~

~~2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,~~

~~2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,~~

~~2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.~~

~~2.3. Level 3:~~

~~2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,~~

~~2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,~~

~~2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.~~

~~2.4. Level 4:~~

~~2.4.1 No cyber security policy exists; or,~~

~~2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,~~

~~2.4.3 No documented change control and configuration management process exists.~~

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to	

		include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-1~~2~~

3. Purpose: Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-004-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-004:~~

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain~~, and document~~ a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

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

R2. Training — The Responsible Entity shall establish, document, implement, and maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the. The cyber security training program shall be reviewed annually, at a minimum, and update asshall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days ofprior to their being granted such authorization.access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program within thirty days ofprior to such personnel being granted such access. Such except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:~~

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. ~~Documentation of the~~The Responsible ~~Entity's~~Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. ~~Documentation~~The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. ~~Documentation~~The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.~~

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~**2.1.1** Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,~~

~~**2.1.2** Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,~~

~~**2.1.3** Personnel risk assessment program exists, but documentation of that program does not exist; or,~~

~~**2.1.4** List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.~~

~~**2.1.5** One personnel risk assessment is not updated at least every seven years, or for cause; or,~~

~~**2.1.6** One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.~~

~~2.2. Level 2:~~

~~**2.2.1** Awareness program does not exist or is not implemented; or,~~

~~**2.2.2** Training program exists, but does not address the requirements identified in Standard CIP-004; or,~~

~~**2.2.3** Personnel risk assessment program exists, but assessments are not conducted as required; or,~~

~~2.2.4 One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.~~

~~2.3. Level 3:~~

~~2.3.1 Training program exists, but has not been reviewed and updated at least annually; or,~~

~~2.3.2 A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,~~

~~2.3.3 List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.~~

~~2.4. Level 4:~~

~~2.4.1 No documented training program exists; or,~~

~~2.4.2 No documented personnel risk assessment program exists; or,~~

~~2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel termination for cause…”	03/24/06
1	06/01/06	D.2.1.4 — Change “access control rights” to “access rights.”	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to	

		clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to “Critical Cyber Assets”. Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

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

2. Number: CIP-005-~~1~~2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations.~~Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-005:~~

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003~~,~~-2; Standard CIP-004-2 Requirement R3~~,~~; Standard CIP-005-2 Requirements R2 and R3~~,~~; Standard CIP-006 ~~Requirements R2 and~~ -2 Requirement R3~~,~~-; Standard CIP-007~~,~~-2 Requirements R1 and R3 through R9~~,~~; Standard CIP-008~~,~~-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; ~~and,~~

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-005.~~ Responsible ~~entities may document controls either individually or by specified applicable grouping.~~

M1. ~~Documents~~ Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. ~~Documentation~~The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. ~~Documentation~~The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. Access The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1. Compliance Enforcement Authority

1.1.1 Regional Reliability Organizations Entity for Responsible Entities.

1.1.1 NERC that do not perform delegated tasks for their Regional Reliability Organization Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The compliance monitor Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records for three years. and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior

manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

~~2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,~~

~~2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,~~

~~2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-1~~2~~

3. Purpose: Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~.~~ ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~ -2.

4. Applicability:

4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-006-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-006:~~

R1. Physical Security Plan — The Responsible Entity shall ~~create~~document, implement, and maintain a physical security plan, approved by ~~a~~ the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. ~~Processes to ensure and document that all~~ All Cyber Assets within an Electronic Security Perimeter ~~also~~ shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the

Responsible Entity shall deploy and document alternative measures to control physical access to ~~the Critical~~such Cyber Assets.

R1.2. ~~Processes to identify all~~Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. ~~Procedures for the appropriate~~Appropriate use of physical access controls as described in Requirement ~~R3~~R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. ~~Procedures for reviewing~~Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. ~~Procedures for~~Continuous escorted access within the ~~physical security perimeter~~Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. ~~Process for updating~~ Update of the physical security plan within ~~ninety~~thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the ~~physical security perimeter~~Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets ~~used in the~~that authorize and/or log access ~~control and monitoring of~~to the Physical Security Perimeter(s~~)~~), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall ~~be~~:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003~~,~~-2; Standard CIP-004-2 Requirement R3~~,~~; Standard CIP-005-2 Requirements R2 and R3~~,~~; Standard CIP-006 ~~Requirement R2 and R3,~~-2 Requirements R4 and R5; Standard CIP-007~~,~~-2; Standard CIP-008-2; and Standard CIP-009-2.

~~**R1.9.** Process for ensuring that the physical security plan is reviewed at least annually.~~

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

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

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3R4, R5, and R4R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance withResponsible Entity shall make available the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. DocumentationThe Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2R4.

M5. DocumentationThe Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R3R5.

M6. DocumentationThe Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R4R6.

M7. AccessThe Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R5R7.

M8. DocumentationThe Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R6.R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1. Compliance Enforcement Authority

1.1.1 Regional Reliability OrganizationsEntity for Responsible Entities.

1.1.1 NERC that do not perform delegated tasks for their Regional Reliability OrganizationEntity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R5R7 and R6R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The compliance monitorCompliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records for three calendar years.and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

2. Violation Severity Levels of Noncompliance

2.1. Level 1:

2. The physical security plan exists, but has not been updated within ninety calendar days of a modification to(Under development by the plan or any of its components; or,CIP VSL Drafting Team)

3.1.1 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

3.1.2 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

3.1.3 Physical access logs are retained for a period shorter than ninety days; or,

3.1.4 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

3.1.5 One required document does not exist.

3.2. Level 2:

3.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

3.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

3.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

3.2.4 More than one required document does not exist.

3.3. Level 3:

~~3.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,~~

~~3.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~3.3.3 No logs of monitored physical access are retained.~~

~~3.4. Level 4:~~

~~3.4.1 No physical security plan exists; or,~~

~~3.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~3.4.3 No maintenance or testing program exists.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance	

		Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~1~~2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):~~

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service

packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish ~~and~~ , document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish ~~and~~ , document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~thirty calendar days of the change being completed.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:~~

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. ~~Documentation~~The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. ~~Documentation and records of the Responsible Entity's~~The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. ~~Documentation~~The Responsible Entity shall make available documentation and records of ~~the Responsible Entity's~~its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. ~~Documentation~~The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.~~

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~**2.1.1** System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or~~

~~**2.1.2** One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,~~

~~**2.1.3** One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,~~

~~**2.1.4** Any one of:~~

- ~~Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,~~
- ~~A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,~~
- ~~Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.~~

~~2.2. Level 2:~~

~~2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.3. Level 3:~~

~~2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4. Level 4:~~

~~2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4.3 No logs exist.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-1~~2~~

3. **Purpose:** Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. **Applicability**

   4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional ~~Reliability Organizations~~Entity.

   4.2. The following are exempt from Standard CIP-008-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. **Effective Date:** ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-008:~~

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident ~~Response~~response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of ~~incident~~Cyber Security Incident response teams, ~~incident~~Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ~~–~~ ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ~~–~~ ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the ~~incident~~Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of CIP-008:~~

M1. ~~The~~ Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. ~~All~~The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.~~

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

~~2. Levels of Noncompliance~~

~~**2.1. Level 1:** A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.~~

~~**2.2. Level 2:**~~

~~**2.2.1** A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,~~

~~**2.2.2** A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,~~

~~**2.2.3** Records related to reportable Cyber Security Incidents were not retained for three calendar years.~~

~~**2.3. Level 3:**~~

~~**2.3.1** A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,~~

~~**2.3.2** A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.~~

~~**2.4. Level 4:** A Cyber Security Incident response plan does not exist.~~

2. **Violation Severity Levels (To be developed later.)**

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-~~1~~2

3. Purpose: Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009~~. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~-2.

4. Applicability:

4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional ~~Reliability Organizations~~Entity

4.2. The following are exempt from Standard CIP-009-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-009:~~

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:~~

M1. ~~Recovery~~Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. ~~Records~~The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. ~~Documentation of~~ The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. ~~Documentation~~The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. ~~Documentation~~The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.34.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.34.2 The Compliance ~~Monitor~~Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.~~

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.~~

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,~~

~~2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.~~

~~2.2. Level 2:~~

~~2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,~~

~~2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.~~

~~2.3. Level 3:~~

~~2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,~~

~~2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.~~

~~2.4. Level 4:~~

~~2.4.1 No recovery plan(s) exist; or,~~

~~2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.~~

2. Violation Severity Levels (To be developed later.)

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	