
**BEFORE THE
NOVA SCOTIA UTILITY AND REVIEW BOARD
OF THE PROVINCE OF NOVA SCOTIA**

**NORTH AMERICAN ELECTRIC)
RELIABILITY CORPORATION)**

**FOURTH QUARTER 2013 APPLICATION
FOR APPROVAL OF RELIABILITY STANDARDS OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION**

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

*Counsel for North American Electric Reliability
Corporation*

February 28, 2014

TABLE OF CONTENTS

I. NOTICES AND COMMUNICATIONS 2

II. REQUEST FOR APPROVAL OF RELIABILITY STANDARDS 2

III. CONCLUSION.....12

EXHIBITS

Exhibit A –

- 1.) NERC Reliability Standards Applicable to Nova Scotia, Approved by FERC in Fourth Quarter 2013
- 2.) PDF Copies of Reliability Standards being filed for approval; and\
- 3.) Updated NERC Glossary of Terms

Exhibit B – Informational Summary of Each Reliability Standard Applicable to Nova Scotia, Approved by FERC in Fourth Quarter 2013

Exhibit C – List of Currently Effective NERC Reliability Standards

**BEFORE THE
NOVA SCOTIA UTILITY AND REVIEW BOARD
OF THE PROVINCE OF NOVA SCOTIA**

NORTH AMERICAN ELECTRIC)
RELIABILITY CORPORATION)

**FOURTH QUARTER 2013 APPLICATION
FOR APPROVAL OF RELIABILITY STANDARDS OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION**

The North American Electric Reliability Corporation (“NERC”) hereby submits to the Nova Scotia Utility and Review Board (“NSUARB”) an application for approval of the NERC Reliability Standards and an updated NERC Glossary of Terms approved by the United States Federal Energy Regulatory Commission (“FERC” or the “Commission”), submitted for informational purposes. This filing covers the time period from October 1, 2013 through December 31, 2013. NERC requests that, as specified herein, these Reliability Standards and Definitions be made mandatory and enforceable for users, owners, and operators of the bulk-power system within the Province of Nova Scotia.

In support of this request for approval of the proposed Reliability Standards and Definitions, NERC submits the following information: (1) Reliability Standards approved by FERC in the fourth quarter of 2013 and the associated updated NERC Glossary of Terms (*see Exhibit A*); (2) an informational summary for each Reliability Standard approved by FERC in the fourth quarter of 2013, including each Standard’s purpose, applicability, and ballot body approval percentages (*see Exhibit B*); and (3) an

updated list of the currently-effective Reliability Standards as approved by FERC (*see Exhibit C*).

I. NOTICES AND COMMUNICATIONS

Notices and communications regarding this Application may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

II. REQUEST FOR APPROVAL OF RELIABILITY STANDARDS

A. Background: NERC Quarterly Filing of Proposed Reliability Standards

On July 20, 2011, NSUARB issued a decision approving the Reliability Standards and NERC Glossary of Terms that NERC submitted to NSUARB on June 30, 2010, and accepted as guidance the Violation Risk Factors (“VRF”) and Violation Severity Levels (“VSL”) associated with the currently-effective Reliability Standards.¹

¹ *In the Matter of an Application by North American Electric Reliability Corporation for Approval of its Reliability Standards, and an application by Northeast Power Coordinating Council, Inc. for Approval of its Regional Reliability Criteria*, NSUARB-NERC-R-10 (July 20, 2011) (“NSUARB Decision”).

NERC has been certified as the Electric Reliability Organization (“ERO”)² in the United States under Section 215 of the Federal Power Act.³ The Reliability Standards contained in **Exhibit A** have been approved as mandatory and enforceable for users, owners, and operators within the United States by FERC.⁴ Some or all of NERC’s Reliability Standards are now mandatory in the Canadian Provinces of Alberta, British Columbia, Manitoba, New Brunswick, Nova Scotia, Ontario, Québec, and Saskatchewan.

NERC entered into a Memorandum of Understanding (“MOU”) with the NSUARB⁵ and a separate MOU with Nova Scotia Power Incorporated (“NSPI”), and the Northeast Power Coordinating Council, Inc. (“NPCC”),⁶ which became effective on December 22, 2006 and May 11, 2010, respectively. The May 11, 2010 MOU sets forth the mutual understandings of NERC, NSPI, and NPCC regarding the approval and implementation of NERC Reliability Standards and NPCC Regional Reliability Criteria in Nova Scotia and other related matters.

In addition, the NSUARB Decision approved a “quarterly review” process for considering new and amended NERC standards and criteria.⁷ On September 2, 2011, NERC submitted its Second Quarter 2011 application filing to NSUARB, in which NERC committed to file a quarterly application with the NSUARB within sixty days

² Through enactment of the Energy Policy Act of 2005, the U.S. Congress entrusted FERC with the duties of approving and enforcing rules in the U.S. to ensure the reliability of the Nation’s bulk power system, and with the duties of certifying an ERO. On July 20, 2006, FERC certified NERC as the ERO, charged with developing mandatory and enforceable Reliability Standards, which are subject to FERC review and approval.

³ 16 U.S.C. § 824o(f) (2006).

⁴ Those standards marked with an asterisk are not yet effective, but have been approved by FERC.

⁵ See Memorandum of Understanding between Nova Scotia Utility and Review Board and North American Electric Reliability Corporation (signed December 22, 2006).

⁶ See Memorandum of Understanding between Nova Scotia Power Incorporated and the Northeast Power Coordinating Council, Inc. and the North American Electric Reliability Corporation (signed May 11, 2010).

⁷ NSUARB Decision at P 30.

after the end of each quarter for approval of all NERC Reliability Standards and updated Glossary of Terms approved by FERC during that quarter.

The NSUARB Decision also determined that quarterly “applications will not be processed by the Board until [FERC] has approved or remanded the standards in the United States.”⁸ Therefore, NERC is only requesting NSUARB approval for those Reliability Standards approved by FERC.

The NSUARB Decision also concluded that NSUARB approval is not required for VRFs and VSLs associated with proposed Reliability Standards.⁹ Thus, NERC does not seek formal approval of VRFs and VSLs associated with the Reliability Standards submitted in this quarterly application. However, because the NSUARB has determined that it will accept the VRFs and VSLs as guidance, NERC is providing a link to the associated FERC-approved VRFs and VSLs for the Reliability Standards for informational purposes.¹⁰

NERC has not included in this filing the full developmental record for the standards, which consists of the draft standards, comments received, responses to the comments by the drafting teams, and the full voting record, because the record for each standard may consist of several thousand pages. NERC will make the full developmental record available to the NSUARB or other interested parties upon request.

⁸ NSUARB Decision at P 30.

⁹ *Id.* at P 33.

¹⁰ NERC’s VRF and VSL matrices are available at:
<http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United States>.
See left-hand side of webpage for downloadable documents.

B. Overview of NERC Reliability Standards Development Process

NERC Reliability Standards define the requirements for reliably planning and operating the North American bulk-power system. These standards are developed by industry stakeholders using a balanced, open, fair and inclusive process managed by the NERC Standards Committee. The Standards Committee is facilitated by NERC staff and comprised of representatives from ten electricity stakeholder segments. Stakeholders, through the balloting process, and the NERC Board of Trustees have approved the standards provided in **Exhibit A**.

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) and Appendix 3A (Standards Processes Manual) of its Rules of Procedure.¹¹ NERC's Reliability Standards development process has been approved by the American National Standards Institute as being open, inclusive, balanced, and fair. The NERC Glossary of Terms used in Reliability Standards – most recently updated November 8, 2013 – lists each term that is defined for use in one or more of NERC's continent-wide or Regional Reliability Standards approved by the NERC Board of Trustees, and is submitted for informational purposes. NERC is requesting approval of three new Definitions included in the Glossary, as detailed below.

C. Description of Proposed Definitions and Reliability Standards, Fourth Quarter 2013

As explained below, six FERC orders were issued in the fourth quarter of 2013 approving NERC Reliability Standards (1) a letter order approving Reliability Standard

¹¹ NERC's Rules of Procedure are available at: <http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx>.

BAL-001-1 issued on October 16, 2013;¹² (2) an order approving the Transmission System Planning Performance Requirements Standard TPL-001-4 issued on October 17, 2013;¹³ (3) an order approving the retirement of 34 requirements within 19 Reliability Standards issued on November 21, 2013;¹⁴ (5) an order approving Version 5 Critical Infrastructure Reliability Standards, CIP-002-5 through CIP-011-1 issued on November 22, 2013;¹⁵ and (6) an order approving Protection System Maintenance Standard PRC-005-2 issued on December 19, 2013.¹⁶

Reliability Standard¹⁷	Effective Date
Resource and Demand Balancing (BAL) Standards	
BAL-001-1*	4/1/2014
Transmission System Planning Performance Requirements (TPL) Standard	
TPL-001-4*	1/1/2015
Cyber Security (CIP) Standards	
CIP-002-5.1*	4/1/2016
CIP-003-5*	4/1/2016
CIP-004-5.1*	4/1/2016
CIP-005-5*	4/1/2016
CIP-006-5*	4/1/2016
CIP-007-5*	4/1/2016
CIP-008-5*	4/1/2016
CIP-009-5*	4/1/2016
CIP-010-1*	4/1/2016
CIP-011-1*	4/1/2016
Protection System Maintenance (PRC) Standard	
PRC-005-2*	4/1/2015

¹² *North American Electric Reliability Corp.*, Docket No. RD13-11-000 (October 16, 2013)(unpublished letter order). The Commission also approved Regional Reliability Standard BAL-004-WECC-02, which does not apply to Nova Scotia.

¹³ *Transmission Planning Reliability Standards*, Order No. 786, 145 FERC ¶ 61,051 (2013).

¹⁴ *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, Order No. 788, 145 FERC ¶ 61,147 (2013).

¹⁵ *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013).

¹⁶ *Protection System Maintenance Reliability Standard*, Order No. 793, 145 FERC ¶ 61,253 (2013).

¹⁷ *At the time of this filing, all standards marked with an asterisk are not yet effective, but have been approved by FERC and have a future mandatory effective date.

Paragraph 81 Requirements Approved for Retirement by FERC – Effective January 21, 2014		
BAL-005-0.2b R2	CIP-003-4 R4.2	INT-007-1 R1.2
CIP-003-3 R1.2	CIP-005-3a R2.6	IRO-016-1 R2
CIP-003-3 R3	CIP-005-4a R2.6	NUC-001-2 R9.1
CIP-003-3 R3.1	CIP-007-3 R7.3	NUC-001-2 R9.1.1
CIP-003-3 R3.2	CIP-007-4 R7.3	NUC-001-2 R9.1.2
CIP-003-3 R3.3	EOP-005-2 R3.1	NUC-001-2 R9.1.3
CIP-003-3 R4.2	FAC-002-1 R2	NUC-001-2 R9.1.4
CIP-003-4 R1.2	FAC-008-3 R4	PRC-010-0 R2
CIP-003-4 R3	FAC-008-3 R5	PRC-022-1 R2
CIP-003-4 R3.1	FAC-010-2.1 R5	VAR-001-2 R5
CIP-003-4 R3.2	FAC-011-2 R5	
CIP-003-4 R3.3	FAC-013-2 R3	

1. BAL-001-1

On October 16, 2013, FERC approved Reliability Standard BAL-001-1- Real Power Balancing Control Performance. Reliability Standard BAL-001-1 maintains Interconnection steady-state frequency within defined limits by balancing power demand and supply in real-time.

2. TPL-001-4

On October 17, 2013, FERC approved Reliability Standard TPL-001-4-Transmission System Planning Performance Requirements. Reliability Standard TPL-001-4 introduces significant revisions and improvements by requiring and improvements by requiring annual

assessments addressing near-term and long-term planning horizons for steady state, short circuit and stability conditions.

3. Paragraph 81 Retirement of Requirements

On March 15, 2012, FERC issued an order¹⁸ on the NERC Find, Fix, Track and Report (“FFT”) program that stated in paragraph 81 (“P 81”):

The Commission notes that NERC’s FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. *If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief.* In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards *unnecessary or redundant* requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

In response to the Commission’s FFT Order and, specifically, the language in P 81, a joint collaborative effort was formed among various industry stakeholders, trade associations, NERC Staff, and Staff from the Regional Entities; this effort became known as “P 81.”¹⁹ The scope of the P 81 project was limited solely to the removal of requirements in their entirety that would not otherwise compromise the integrity of the specific Reliability Standard or impact the reliability of the BES. The criteria developed by the P 81 Team were designed so that no

¹⁸ *North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 at P 81 (2012)(emphasis added)(“FFT Order”).

¹⁹ **Exhibit G** contains a list of the Project 2013-02 team members (“P 81 Team”).

rewriting or consolidation of requirements would be necessary. The P 81 Team developed three criteria: (1) Criteria A: an overarching criteria designed to determine that there is no reliability gap created by the proposed retirement; (2) Criteria B: consists of seven separate identifying criteria designed to recognize requirements appropriate for retirement (administrative; data collection/data retention; documentation; reporting; periodic updates; commercial or business practice; and redundant); and (3) Criteria C: consists of seven separate questions designed to assist the P 81 Team in making an informed decision regarding whether requirements are appropriate to propose for retirement.²⁰

On November 21, 2013, FERC approved the retirement of 34 requirements within 19 Reliability Standards. The requirements proposed for retirement either: (1) provide little protection for Bulk-Power System reliability or (2) are redundant with other aspects of the Reliability Standards. No Reliability Standards were proposed for retirement in entirety, and all other requirements in each of the affected Reliability Standards will remain in continuous effect. The version numbers of the affected Reliability Standards were not incremented, but the retired requirements and associated elements are clearly marked as “retired.”²¹

²⁰ C1: Was the Reliability Standard requirement part of a FFT filing?
C2: Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?
C3: What is the VRF of the Reliability Standard requirement?
C4: In which tier of the 2013 AML does the Reliability Standard requirement fall?
C5: Is there a possible negative impact on NERC’s published and posted reliability principles?
C6: Is there any negative impact on the defense in depth protection of the Bulk Electric System?
C7: Does the retirement promote results or performance based Reliability Standards?

²¹ Given that only individual Requirements are affected by the P 81 initiative, informational summary sheets for these Reliability Standards are not included in Exhibit B, but are included in Exhibit A.

4. Version 5 Critical Infrastructure Reliability Standards

On November 22, 2013, FERC approved the Version 5 Critical Infrastructure Protection Reliability Standards, CIP-002-5 through CIP-011-1 (“CIP Version 5”). The CIP version 5 Standards address the cyber security of the bulk electric system. The CIP version 5 Standards adopt new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards.

FERC also approved nineteen new or revised definitions associated with the CIP version 5 Standards for inclusion in the *Glossary of Terms Used in NERC Reliability Standards*. The new definitions are as follows: (1) BES Cyber Asset, (2) BES Cyber System, (3) BES Cyber System Information, (4) CIP Exceptional Circumstance, (5) CIP Senior Manager, (6) Control Center, (7) Dial-up Connectivity, (8) Electronic Access Control or Monitoring Systems, (9) Electronic Access Point, (10) External Routable Connectivity, (11) Intermediate System, (12) Physical Access Control Systems, (13) Protected Cyber Assets, (14) Interactive Remote Access, and (15) Reportable Cyber Security Incident. The revised definitions are as follows: (1) Cyber Assets, (2) Cyber Security Incident, (3) Electronic Security Perimeter, and (4) Physical Security Perimeter.

In Order No. 791, FERC directed modifications to the CIP version 5 Standards. FERC directed NERC to remove language found in 17 requirements in the CIP version 5 Standards that requires responsible entities to implement the requirements in a manner to “identify, assess, and correct” deficiencies by February 3, 2015 (one year from the effective date of Order No. 791).²² FERC also noted that the CIP version 5 Standards do not require specific controls for Low Impact assets nor do they contain objective criteria from which to judge the

²² Order No. 791 at P 4.

sufficiency of the controls ultimately adopted by responsible entities for Low Impact assets. FERC directed NERC to develop modifications to the CIP version 5 Standards to address this concern.²³ NERC has initiated a project to address these revisions.²⁴

5. PRC-005-2

On December 19, 2013, FERC approved Reliability Standard PRC-005-2 and six associated definitions, Component, Component Type, Countable Event, Protection System Maintenance Program, Segment, and Unresolved Maintenance Issue. Of these newly defined terms, only the term “Protection System Maintenance Program” was incorporated into NERC’s Glossary of Terms, with the remainder applying only to Reliability Standard PRC-005-2.

Reliability Standard PRC-005-2 represents an improvement over the four existing standards covering protection system maintenance and testing,²⁵ by incorporating specific, required minimum maintenance activities and maximum time intervals for maintenance of individual components of protection systems and load shedding equipment affecting the bulk electric system.

²³ Order No. 791 at P 5.

²⁴ Project 2014-02, *available at*: <http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx>.

²⁵ PRC-005-1.1b (Transmission and Generation Protection System Maintenance and Testing), PRC-008-0 (Underfrequency Load Shedding Equipment Maintenance), PRC-011-0 (Undervoltage Load Shedding Equipment Maintenance) and PRC-017-0 (Special Protection System Maintenance and Testing).

III. CONCLUSION

NERC respectfully requests that the NSUARB approve the Reliability Standards and Definitions as specified herein.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

/s/ Stacey Tyrewala
Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

*Counsel for North American Electric Reliability
Corporation*

EXHIBIT A(1): NERC Reliability Standards Applicable to Nova Scotia, Approved by FERC in Fourth Quarter 2013

Reliability Standard	Effective Date
Resource and Demand Balancing (BAL) Standards	
BAL-001-1*	4/1/2014
Transmission System Planning Performance Requirements (TPL) Standard	
TPL-001-4*	1/1/2015
Cyber Security (CIP) Standards	
CIP-002-5.1*	4/1/2016
CIP-003-5*	4/1/2016
CIP-004-5.1*	4/1/2016
CIP-005-5*	4/1/2016
CIP-006-5*	4/1/2016
CIP-007-5*	4/1/2016
CIP-008-5*	4/1/2016
CIP-009-5*	4/1/2016
CIP-010-1*	4/1/2016
CIP-011-1*	4/1/2016
Protection System Maintenance (PRC) Standard	
PRC-005-2*	4/1/2015

*At the time of this filing, all standards marked with an asterisk are not yet effective, but have been approved by FERC and have a future mandatory effective date.

Exhibit A(2): PDF Copies of Reliability Standards being Filed for Approval

A. Introduction

1. **Title:** Real Power Balancing Control Performance
2. **Number:** BAL-001-1
3. **Purpose:** To maintain Interconnection steady-state frequency within defined limits by balancing real power demand and supply in real-time.
4. **Applicability:**
 - 4.1. Balancing Authorities
5. **Effective Date:** The WECC Regional Variance to NERC Reliability Standard BAL-001-1 is to be effective on the first day of the second quarter, after regulatory approval.

B. Requirements

- R1.** Each Balancing Authority shall operate such that, on a rolling 12-month basis, the average of the clock-minute averages of the Balancing Authority's Area Control Error (ACE) divided by 10B (B is the clock-minute average of the Balancing Authority Area's Frequency Bias) times the corresponding clock-minute averages of the Interconnection's Frequency Error is less than a specific limit. This limit ϵ_1^2 is a constant derived from a targeted frequency bound (separately calculated for each Interconnection) that is reviewed and set as necessary by the NERC Operating Committee.

$$AVG_{Period} \left[\left(\frac{ACE_i}{-10B_i} \right)_1 * \Delta F_1 \right] \leq \epsilon_1^2 \text{ or } \frac{AVG_{Period} \left[\left(\frac{ACE_i}{-10B_i} \right)_1 * \Delta F_1 \right]}{\epsilon_1^2} \leq 1$$

The equation for ACE is:

$$ACE = (NI_A - NI_S) - 10B (F_A - F_S) - I_{ME}$$

where:

- NI_A is the algebraic sum of actual flows on all tie lines.
 - NI_S is the algebraic sum of scheduled flows on all tie lines.
 - B is the Frequency Bias Setting (MW/0.1 Hz) for the Balancing Authority. The constant factor 10 converts the frequency setting to MW/Hz.
 - F_A is the actual frequency.
 - F_S is the scheduled frequency. F_S is normally 60 Hz but may be offset to effect manual time error corrections.
 - I_{ME} is the meter error correction factor typically estimated from the difference between the integrated hourly average of the net tie line flows (NI_A) and the hourly net interchange demand measurement (megawatt-hour). This term should normally be very small or zero.
- R2.** Each Balancing Authority shall operate such that its average ACE for at least 90% of clock-ten-minute periods (6 non-overlapping periods per hour) during a calendar month is within a specific limit, referred to as L_{10} .

$$AVG_{10\text{-minute}} (ACE_i) \leq L_{10}$$

where:

$$L_{10} = 1.65 \in_{10} \sqrt{(-10B_i)(-10B_s)}$$

ϵ_{10} is a constant derived from the targeted frequency bound. It is the targeted root-mean-square (RMS) value of ten-minute average Frequency Error based on frequency performance over a given year. The bound, ϵ_{10} , is the same for every Balancing Authority Area within an Interconnection, and B_s is the sum of the Frequency Bias Settings of the Balancing Authority Areas in the respective Interconnection. For Balancing Authority Areas with variable bias, this is equal to the sum of the minimum Frequency Bias Settings.

- R3.** Each Balancing Authority providing Overlap Regulation Service shall evaluate Requirement R1 (i.e., Control Performance Standard 1 or CPS1) and Requirement R2 (i.e., Control Performance Standard 2 or CPS2) using the characteristics of the combined ACE and combined Frequency Bias Settings.
- R4.** Any Balancing Authority receiving Overlap Regulation Service shall not have its control performance evaluated (i.e. from a control performance perspective, the Balancing Authority has shifted all control requirements to the Balancing Authority providing Overlap Regulation Service).

C. Measures

- M1.** Each Balancing Authority shall achieve, as a minimum, Requirement 1 (CPS1) compliance of 100%.

CPS1 is calculated by converting a compliance ratio to a compliance percentage as follows:

$$CPS1 = (2 - CF) * 100\%$$

The frequency-related compliance factor, CF, is a ratio of all one-minute compliance parameters accumulated over 12 months divided by the target frequency bound:

$$CF = \frac{CF_{12\text{-month}}}{(\epsilon_1)^2}$$

where: ϵ_1 is defined in Requirement R1.

The rating index $CF_{12\text{-month}}$ is derived from 12 months of data. The basic unit of data comes from one-minute averages of ACE, Frequency Error and Frequency Bias Settings.

A clock-minute average is the average of the reporting Balancing Authority's valid measured variable (i.e., for ACE and for Frequency Error) for each sampling cycle during a given clock-minute.

$$\left(\frac{ACE}{-10B} \right)_{\text{clock-minute}} = \frac{\left(\frac{\sum ACE_{\text{sampling cycles in clock-minute}}}{n_{\text{sampling cycles in clock-minute}}} \right)}{-10B}$$

$$\Delta F_{\text{clock-minute}} = \frac{\sum \Delta F_{\text{sampling cycles in clock-minute}}}{n_{\text{sampling cycles in clock-minute}}}$$

The Balancing Authority's clock-minute compliance factor (CF) becomes:

$$CF_{\text{clock-minute}} = \left[\left(\frac{ACE}{-10B} \right)_{\text{clock-minute}} * \Delta F_{\text{clock-minute}} \right]$$

Normally, sixty (60) clock-minute averages of the reporting Balancing Authority’s ACE and of the respective Interconnection’s Frequency Error will be used to compute the respective hourly average compliance parameter.

$$CF_{\text{clock-hour}} = \frac{\sum CF_{\text{clock-minute}}}{n_{\text{clock-minute samples in hour}}}$$

The reporting Balancing Authority shall be able to recalculate and store each of the respective clock-hour averages (CF clock-hour average-month) as well as the respective number of samples for each of the twenty-four (24) hours (one for each clock-hour, i.e., hour-ending (HE) 0100, HE 0200, ..., HE 2400).

$$CF_{\text{clock-hour average-month}} = \frac{\sum_{\text{days-in-month}} [(CF_{\text{clock-hour}})(n_{\text{one-minute samples in clock-hour}})]}{\sum_{\text{days-in month}} [n_{\text{one-minute samples in clock-hour}}]}$$

$$CF_{\text{month}} = \frac{\sum_{\text{hours-in-day}} [(CF_{\text{clock-hour average-month}})(n_{\text{one-minute samples in clock-hour averages}})]}{\sum_{\text{hours-in day}} [n_{\text{one-minute samples in clock-hour averages}}]}$$

The 12-month compliance factor becomes:

$$CF_{12\text{-month}} = \frac{\sum_{i=1}^{12} (CF_{\text{month-}i})(n_{(\text{one-minute samples in month-}i)})}{\sum_{i=1}^{12} [n_{(\text{one-minute samples in month-}i)}]}$$

In order to ensure that the average ACE and Frequency Deviation calculated for any one-minute interval is representative of that one-minute interval, it is necessary that at least 50% of both ACE and Frequency Deviation samples during that one-minute interval be present. Should a sustained interruption in the recording of ACE or Frequency Deviation due to loss of telemetering or computer unavailability result in a one-minute interval not containing at least 50% of samples of both ACE and Frequency Deviation, that one-minute interval shall be excluded from the calculation of CPS1.

- M2.** Each Balancing Authority shall achieve, as a minimum, Requirement R2 (CPS2) compliance of 90%. CPS2 relates to a bound on the ten-minute average of ACE. A compliance percentage is calculated as follows:

$$CPS2 = \left[1 - \frac{\text{Violations}_{\text{month}}}{(\text{Total Periods}_{\text{month}} - \text{Unavailable Periods}_{\text{month}})} \right] * 100$$

The violations per month are a count of the number of periods that ACE clock-ten-minutes exceeded L₁₀. ACE clock-ten-minutes is the sum of valid ACE samples within a clock-ten-minute period divided by the number of valid samples.

Violation clock-ten-minutes

$$= 0 \text{ if } \left| \frac{\sum ACE}{n_{\text{samples in 10-minutes}}} \right| \leq L_{10}$$

$$= 1 \text{ if } \left| \frac{\sum ACE}{n_{\text{samples in 10-minutes}}} \right| > L_{10}$$

Each Balancing Authority shall report the total number of violations and unavailable periods for the month. L_{10} is defined in Requirement R2.

Since CPS2 requires that ACE be averaged over a discrete time period, the same factors that limit total periods per month will limit violations per month. The calculation of total periods per month and violations per month, therefore, must be discussed jointly.

A condition may arise which may impact the normal calculation of total periods per month and violations per month. This condition is a sustained interruption in the recording of ACE.

In order to ensure that the average ACE calculated for any ten-minute interval is representative of that ten-minute interval, it is necessary that at least half the ACE data samples are present for that interval. Should half or more of the ACE data be unavailable due to loss of telemetering or computer unavailability, that ten-minute interval shall be omitted from the calculation of CPS2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

One calendar month.

1.3. Data Retention

The data that supports the calculation of CPS1 and CPS2 (Appendix 1-BAL-001-0) are to be retained in electronic form for at least a one-year period. If the CPS1 and CPS2 data for a Balancing Authority Area are undergoing a review to address a question that has been raised regarding the data, the data are to be saved beyond the normal retention period until the question is formally resolved. Each Balancing Authority shall retain for a rolling 12-month period the values of: one-minute average ACE (ACE_t), one-minute average Frequency Error, and, if using variable bias, one-minute average Frequency Bias.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance – CPS1

2.1. Level 1: The Balancing Authority Area's value of CPS1 is less than 100% but greater than or equal to 95%.

2.2. Level 2: The Balancing Authority Area's value of CPS1 is less than 95% but greater than or equal to 90%.

2.3. Level 3: The Balancing Authority Area’s value of CPS1 is less than 90% but greater than or equal to 85%.

2.4. Level 4: The Balancing Authority Area’s value of CPS1 is less than 85%.

3. Levels of Non-Compliance – CPS2

3.1. Level 1: The Balancing Authority Area’s value of CPS2 is less than 90% but greater than or equal to 85%.

3.2. Level 2: The Balancing Authority Area’s value of CPS2 is less than 85% but greater than or equal to 80%.

3.3. Level 3: The Balancing Authority Area’s value of CPS2 is less than 80% but greater than or equal to 75%.

3.4. Level 4: The Balancing Authority Area’s value of CPS2 is less than 75%.

E. Regional Differences

E.A. The [ERCOT Control Performance Standard 2 Waiver](#) approved November 21, 2002.

E.B. Regional Variance for the Western Electricity Coordinating Council

The following Interconnection-wide variance shall be applicable in the Western Interconnection and replaces, in their entirety, Requirement R1 and Section D.2. (i.e., under Compliance replace Levels of Non-Compliance – CPS1). Please note that the ACE equation is replaced in its entirety with the following equation identified in Requirement E.B.1.

Requirements and Measures

E.B.1. Each Balancing Authority shall operate such that, on a rolling 12-month basis, the average of the clock-minute averages of the Balancing Authority’s Area Control Error (ACE) divided by 10B (B is the clock-minute average of the Balancing Authority Area’s Frequency Bias) times the corresponding clock-minute averages of the Interconnection’s Frequency Error is less than a specific limit. This limit ϵ_1^2 is a constant derived from a targeted frequency bound (separately calculated for each Interconnection) that is reviewed and set as necessary by the NERC Operating Committee.

$$AVG_{Period} \left[\left(\frac{ACE_i}{-10B_i} \right)_1 * \Delta F_1 \right] \leq \epsilon_1^2 \text{ or } \frac{AVG_{Period} \left[\left(\frac{ACE_i}{-10B_i} \right)_1 * \Delta F_1 \right]}{\epsilon_1^2} \leq 1$$

The equation for ACE in the Western Interconnection is:

$$ACE = (NI_A - NI_S) - 10B(F_A - F_S) - I_{ME} + I_{ATEC}$$

where:

- NI_A is the algebraic sum of actual flows on all tie lines.
- NI_S is the algebraic sum of scheduled flows on all tie lines.

- B is the Frequency Bias Setting (MW/0.1 Hz) for the Balancing Authority. The constant factor 10 converts the frequency setting to MW/Hz.
- F_A is the actual frequency.
- F_S is the scheduled frequency. F_S is normally 60 Hz but may be offset to effect manual time error corrections.
- I_{ME} is the meter error correction factor typically estimated from the difference between the integrated hourly average of the net tie line flows (NI_A) and the hourly net interchange demand measurement (megawatt-hour). This term should normally be very small or zero.

$$I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)*H} \text{ when operating in Automatic Time Error Correction control mode.}$$

I_{ATEC} shall be zero when operating in any other AGC mode.

- $Y = B / B_S$.
- H = Number of Hours used to payback Primary Inadvertent Interchange energy. The value of H is set to 3.
- B_S = Frequency Bias for the Interconnection (MW / 0.1 Hz).
- Primary Inadvertent Interchange (PII_{hourly}) is $(1-Y) * (II_{actual} - B * \Delta TE/6)$
- II_{actual} is the hourly Inadvertent Interchange for the last hour.
- ΔTE is the hourly change in system Time Error as distributed by the Interconnection Time Monitor. Where:

$$\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - (t)*(TE_{offset})$$
- TD_{adj} is the Reliability Coordinator adjustment for differences with Interconnection Time Monitor control center clocks.
- t is the number of minutes of Manual Time Error Correction that occurred during the hour.
- TE_{offset} is 0.000 or +0.020 or -0.020.
- PII_{accum} is the Balancing Authority's accumulated PII_{hourly} in MWh. An On-Peak and Off-Peak accumulation accounting is required.

Where:

$$PII_{accum}^{on/off\ peak} = \text{last period's } PII_{accum}^{on/off\ peak} + PII_{hourly}$$

[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]

- M.E.B.1.** Each Balancing Authority shall achieve, as a minimum, Requirement E.B.1 (CPS1) compliance of 100%.

CPS1 is calculated by converting a compliance ratio to a compliance percentage as follows:

$$CPS1 = (2 - CF) * 100\%$$

The frequency-related compliance factor, CF, is a ratio of all one-minute compliance parameters accumulated over 12 months divided by the target frequency bound:

$$CF = \frac{CF_{12\text{-month}}}{(\epsilon_1)^2}$$

where: ϵ_1 is defined in Requirement E.B.1.

The rating index $CF_{12\text{-month}}$ is derived from 12 months of data. The basic unit of data comes from one-minute averages of ACE, Frequency Error and Frequency Bias Settings.

A clock-minute average is the average of the reporting Balancing Authority's valid measured variable (i.e., for ACE and for Frequency Error) for each sampling cycle during a given clock-minute.

$$\left(\frac{ACE}{-10B} \right)_{\text{clock-minute}} = \frac{\left(\frac{\sum ACE_{\text{sampling cycles in clock-minute}}}{n_{\text{sampling cycles in clock-minute}}} \right)}{-10B}$$

$$\Delta F_{\text{clock-minute}} = \frac{\sum \Delta F_{\text{sampling cycles in clock-minute}}}{n_{\text{sampling cycles in clock-minute}}}$$

The Balancing Authority's clock-minute compliance factor (CF) becomes:

$$CF_{\text{clock-minute}} = \left[\left(\frac{ACE}{-10B} \right)_{\text{clock-minute}} * \Delta F_{\text{clock-minute}} \right]$$

Normally, sixty (60) clock-minute averages of the reporting Balancing Authority's ACE and of the respective Interconnection's Frequency Error will be used to compute the respective hourly average compliance parameter.

$$CF_{\text{clock-hour}} = \frac{\sum CF_{\text{clock-minute}}}{n_{\text{clock-minute samples in hour}}}$$

The reporting Balancing Authority shall be able to recalculate and store each of the respective clock-hour averages ($CF_{\text{clock-hour}}$ average-month) as well as the respective number of samples for each of the twenty-four (24) hours (one for each clock-hour, i.e., hour-ending (HE) 0100, HE 0200, ..., HE 2400).

$$CF_{\text{clock-hour average-month}} = \frac{\sum_{\text{days-in-month}} [(CF_{\text{clock-hour}})(n_{\text{one-minute samples in clock-hour}})]}{\sum_{\text{days-in month}} [n_{\text{one-minute samples in clock-hour}}]}$$

$$CF_{\text{month}} = \frac{\sum_{\text{hours-in-day}} [(CF_{\text{clock-hour average-month}})(n_{\text{one-minute samples in clock-hour averages}})]}{\sum_{\text{hours-in day}} [n_{\text{one-minute samples in clock-hour averages}}]}$$

The 12-month compliance factor becomes:

$$CF_{12\text{-month}} = \frac{\sum_{i=1}^{12} (CF_{\text{month-}i})(n_{(\text{one-minute samples in month-}i)})}{\sum_{i=1}^{12} [n_{(\text{one-minute samples in month-}i)}]}$$

In order to ensure that the average ACE and Frequency Deviation calculated for any one-minute interval is representative of that one-minute interval, it is necessary that at least 50% of both ACE and Frequency Deviation samples during that one-minute interval be present. Should a sustained interruption in the recording of ACE or Frequency Deviation due to loss of telemetering or computer unavailability result in a one-minute interval not containing at least 50% of samples of both ACE and Frequency Deviation, that one-minute interval shall be excluded from the calculation of CPS1.

- E.B.2.** Each Balancing Authority shall limit the absolute value of I_{ATEC} , the Automatic Time Error Correction term as follows: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

$$|I_{ATEC}| \leq L_{max}$$

- M.E.B.2.** Forms of acceptable evidence for Requirement E.B.2 may include, but are not limited to:

- Dated Energy Management System (EMS) displays,
- WECC Interchange Tool, EMS application code, or
- Other archived data that demonstrates compliance.

- E.B.3.** Each Balancing Authority shall set L_{max} within the limits as follows:

$$0.20 * |B| \leq L_{max} \leq L_{10}$$

[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

- M.E.B.3.** Forms of acceptable evidence for Requirement E.B.3 may include, but is not limited to:

- Dated Energy Management System (EMS) displays,
- WECC Interchange Tool, EMS application code, or
- Other archived data that demonstrates compliance.

E.B Compliance

1. Evidence Retention

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

Each Balancing Authority in the Western Interconnection shall retain the values of I_{ATEC} and L_{max} for the preceding calendar year (January – December), as well as the current calendar year.

Table of Compliance Elements

E #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
E.B.1	Real-time Operations	Medium	The Balancing Authority Area's value of CPS1 was less than 100% but greater than or equal to 95%.	The Balancing Authority Area's value of CPS1 was less than 95% but greater than or equal to 90%.	The Balancing Authority Area's value of CPS1 was less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS1 was less than 85%.
E.B.2	Real-time Operations	Medium	N/A	N/A	N/A	The Balancing Authority Area's absolute value for I_{ATEC} was greater than L_{max} .
E.B.3	Operations Planning	Medium	N/A	N/A	N/A	The Balancing Authority did not set L_{max} to within the limits in E.B.3 (i.e., $0.20 * B \leq L_{max} \leq L_{10}$).

F. Associated Documents**Version History**

Version	Date	Action	Change Tracking
0	February 8, 2005	BOT Approval	New
0	April 1, 2005	Effective Implementation Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
0	July 24, 2007	Corrected R3 to reference M1 and M2 instead of R1 and R2	Errata
0a	December 19, 2007	Added Appendix 2 – Interpretation of R1 approved by BOT on October 23, 2007	Revised
0a	January 16, 2008	In Section A.2., Added “a” to end of standard number In Section F, corrected automatic numbering from “2” to “1” and removed “approved” and added parenthesis to “(October 23, 2007)”	Errata
0	January 23, 2008	Reversed errata change from July 24, 2007	Errata
0.1a	October 29, 2008	Board approved errata changes; updated version number to “0.1a”	Errata
0.1a	May 13, 2009	Approved by FERC	
1	December 19, 2012	Adopted by NERC Board of Trustees	
1	October 16, 2013	A FERC Letter Order was issued on October 16, 2013, approving BAL-001-1. This standard will become enforceable on April 1, 2014.	

**Appendix 1-BAL-001-1
CPS1 and CPS2 Data**

CPS1 DATA	Description	Retention Requirements
ε_1	A constant derived from the targeted frequency bound. This number is the same for each Balancing Authority Area in the Interconnection.	Retain the value of ε_1 used in CPS1 calculation.
ACE_i	The clock-minute average of ACE.	Retain the 1-minute average values of ACE (525,600 values).
B_i	The Frequency Bias of the Balancing Authority Area.	Retain the value(s) of B_i used in the CPS1 calculation.
F_A	The actual measured frequency.	Retain the 1-minute average frequency values (525,600 values).
F_S	Scheduled frequency for the Interconnection.	Retain the 1-minute average frequency values (525,600 values).

CPS2 DATA	Description	Retention Requirements
V	Number of incidents per hour in which the absolute value of ACE clock-ten-minutes is greater than L_{10} .	Retain the values of V used in CPS2 calculation.
ε_{10}	A constant derived from the frequency bound. It is the same for each Balancing Authority Area within an Interconnection.	Retain the value of ε_{10} used in CPS2 calculation.
B_i	The Frequency Bias of the Balancing Authority Area.	Retain the value of B_i used in the CPS2 calculation.
B_s	The sum of Frequency Bias of the Balancing Authority Areas in the respective Interconnection. For systems with variable bias, this is equal to the sum of the minimum Frequency Bias Setting.	Retain the value of B_s used in the CPS2 calculation. Retain the 1-minute minimum bias value (525,600 values).
U	Number of unavailable ten-minute periods per hour used in calculating CPS2.	Retain the number of 10-minute unavailable periods used in calculating CPS2 for the reporting period.

Guidance and Rationale

Rationale for E.B.1

Premise: When a Balancing Authority Area uses the ACE equation with an ATEC correction component for both control and assessing performance, it provides a more accurate measurement of the Control Performance methodology while at the same time achieving the same reliability objective as the existing BAL-001-0.1a standard.

Justification: Adding the I_{ATEC} term to the ACE equation reduces the number of manual time error corrections and PII_{accum} .

Goal: To establish an ACE equation that permits the implementation of Automatic Time Error Correction.

Rationale for E.B.2

Premise: I_{ATEC} greater than L_{max} may result in a risk to reliability caused by large ATEC payback.

Justification: Balancing Authorities should not control their Balancing Authority Areas using an approach that puts system reliability at risk.

Goal: The goal of Requirement E.B.2 is to limit I_{ATEC} to L_{max} in order to reduce potential reliability risks to the interconnection caused by a large ATEC payback term.

Rationale for E.B.3

Premise: Operating within an L_{max} less than $0.20 * |B|$ may not provide sufficient correction for PII and operating with an L_{max} greater than L_{10} may result in potential reliability risks caused by a large ATEC payback term.

Justification: L_{max} should be limited to prevent Balancing Authorities from creating potential reliability risks caused by a large ATEC payback term.

Goal: The goal of Requirement E.B.3 is to develop a range for L_{max} where Balancing Authorities reduce potential reliability risks by limiting I_{ATEC} to L_{max} .

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard BAL-001-1 — Real Power Balancing Control Performance

United States

Standard	Requirement	Enforcement Date	Inactive Date
BAL-001-1	All	04/01/2014	

A. Introduction

1. **Title:** Transmission System Planning Performance Requirements
2. **Number:** TPL-001-4
3. **Purpose:** Establish Transmission system planning performance requirements within the planning horizon to develop a Bulk Electric System (BES) that will operate reliably over a broad spectrum of System conditions and following a wide range of probable Contingencies.
4. **Applicability:**
 - 4.1. **Functional Entity**
 - 4.1.1. Planning Coordinator.
 - 4.1.2. Transmission Planner.
5. **Effective Date:** Requirements R1 and R7 as well as the definitions shall become effective on the first day of the first calendar quarter, 12 months after applicable regulatory approval. In those jurisdictions where regulatory approval is not required, Requirements R1 and R7 become effective on the first day of the first calendar quarter, 12 months after Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Except as indicated below, Requirements R2 through R6 and Requirement R8 shall become effective on the first day of the first calendar quarter, 24 months after applicable regulatory approval. In those jurisdictions where regulatory approval is not required, all requirements, except as noted below, go into effect on the first day of the first calendar quarter, 24 months after Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

For 84 calendar months beginning the first day of the first calendar quarter following applicable regulatory approval, or in those jurisdictions where regulatory approval is not required on the first day of the first calendar quarter 84 months after Board of Trustees adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, Corrective Action Plans applying to the following categories of Contingencies and events identified in TPL-001-4, Table 1 are allowed to include Non-Consequential Load Loss and curtailment of Firm Transmission Service (in accordance with Requirement R2, Part 2.7.3.) that would not otherwise be permitted by the requirements of TPL-001-4:

- P1-2 (for controlled interruption of electric supply to local network customers connected to or supplied by the Faulted element)
- P1-3 (for controlled interruption of electric supply to local network customers connected to or supplied by the Faulted element)
- P2-1
- P2-2 (above 300 kV)
- P2-3 (above 300 kV)
- P3-1 through P3-5
- P4-1 through P4-5 (above 300 kV)
- P5 (above 300 kV)

B. Requirements

- R1.** Each Transmission Planner and Planning Coordinator shall maintain System models within its respective area for performing the studies needed to complete its Planning Assessment. The models shall use data consistent with that provided in accordance with the MOD-010 and MOD-012 standards, supplemented by other sources as needed, including items represented in the Corrective Action Plan, and shall represent projected System conditions. This establishes Category P0 as the normal System condition in Table 1. *[Violation Risk Factor: Medium]*
[Time Horizon: Long-term Planning]
- 1.1.** System models shall represent:
- 1.1.1. Existing Facilities
 - 1.1.2. Known outage(s) of generation or Transmission Facility(ies) with a duration of at least six months.
 - 1.1.3. New planned Facilities and changes to existing Facilities
 - 1.1.4. Real and reactive Load forecasts
 - 1.1.5. Known commitments for Firm Transmission Service and Interchange
 - 1.1.6. Resources (supply or demand side) required for Load
- R2.** Each Transmission Planner and Planning Coordinator shall prepare an annual Planning Assessment of its portion of the BES. This Planning Assessment shall use current or qualified past studies (as indicated in Requirement R2, Part 2.6), document assumptions, and document summarized results of the steady state analyses, short circuit analyses, and Stability analyses. *[Violation Risk Factor: High]* *[Time Horizon: Long-term Planning]*
- 2.1.** For the Planning Assessment, the Near-Term Transmission Planning Horizon portion of the steady state analysis shall be assessed annually and be supported by current annual studies or qualified past studies as indicated in Requirement R2, Part 2.6. Qualifying studies need to include the following conditions:
- 2.1.1. System peak Load for either Year One or year two, and for year five.
 - 2.1.2. System Off-Peak Load for one of the five years.
 - 2.1.3. P1 events in Table 1, with known outages modeled as in Requirement R1, Part 1.1.2, under those System peak or Off-Peak conditions when known outages are scheduled.
 - 2.1.4. For each of the studies described in Requirement R2, Parts 2.1.1 and 2.1.2, sensitivity case(s) shall be utilized to demonstrate the impact of changes to the basic assumptions used in the model. To accomplish this, the sensitivity analysis in the Planning Assessment must vary one or more of the following conditions by a sufficient amount to stress the System within a range of credible conditions that demonstrate a measurable change in System response :
 - Real and reactive forecasted Load.
 - Expected transfers.
 - Expected in service dates of new or modified Transmission Facilities.
 - Reactive resource capability.
 - Generation additions, retirements, or other dispatch scenarios.

- Controllable Loads and Demand Side Management.
 - Duration or timing of known Transmission outages.
- 2.1.5. When an entity's spare equipment strategy could result in the unavailability of major Transmission equipment that has a lead time of one year or more (such as a transformer), the impact of this possible unavailability on System performance shall be studied. The studies shall be performed for the P0, P1, and P2 categories identified in Table 1 with the conditions that the System is expected to experience during the possible unavailability of the long lead time equipment.
- 2.2.** For the Planning Assessment, the Long-Term Transmission Planning Horizon portion of the steady state analysis shall be assessed annually and be supported by the following annual current study, supplemented with qualified past studies as indicated in Requirement R2, Part 2.6:
- 2.2.1. A current study assessing expected System peak Load conditions for one of the years in the Long-Term Transmission Planning Horizon and the rationale for why that year was selected.
- 2.3.** The short circuit analysis portion of the Planning Assessment shall be conducted annually addressing the Near-Term Transmission Planning Horizon and can be supported by current or past studies as qualified in Requirement R2, Part 2.6. The analysis shall be used to determine whether circuit breakers have interrupting capability for Faults that they will be expected to interrupt using the System short circuit model with any planned generation and Transmission Facilities in service which could impact the study area.
- 2.4.** For the Planning Assessment, the Near-Term Transmission Planning Horizon portion of the Stability analysis shall be assessed annually and be supported by current or past studies as qualified in Requirement R2, Part 2.6. The following studies are required:
- 2.4.1. System peak Load for one of the five years. System peak Load levels shall include a Load model which represents the expected dynamic behavior of Loads that could impact the study area, considering the behavior of induction motor Loads. An aggregate System Load model which represents the overall dynamic behavior of the Load is acceptable.
- 2.4.2. System Off-Peak Load for one of the five years.
- 2.4.3. For each of the studies described in Requirement R2, Parts 2.4.1 and 2.4.2, sensitivity case(s) shall be utilized to demonstrate the impact of changes to the basic assumptions used in the model. To accomplish this, the sensitivity analysis in the Planning Assessment must vary one or more of the following conditions by a sufficient amount to stress the System within a range of credible conditions that demonstrate a measurable change in performance:
- Load level, Load forecast, or dynamic Load model assumptions.
 - Expected transfers.
 - Expected in service dates of new or modified Transmission Facilities.
 - Reactive resource capability.
 - Generation additions, retirements, or other dispatch scenarios.

- 2.5.** For the Planning Assessment, the Long-Term Transmission Planning Horizon portion of the Stability analysis shall be assessed to address the impact of proposed material generation additions or changes in that timeframe and be supported by current or past studies as qualified in Requirement R2, Part 2.6 and shall include documentation to support the technical rationale for determining material changes.
- 2.6.** Past studies may be used to support the Planning Assessment if they meet the following requirements:
- 2.6.1. For steady state, short circuit, or Stability analysis: the study shall be five calendar years old or less, unless a technical rationale can be provided to demonstrate that the results of an older study are still valid.
- 2.6.2. For steady state, short circuit, or Stability analysis: no material changes have occurred to the System represented in the study. Documentation to support the technical rationale for determining material changes shall be included.
- 2.7.** For planning events shown in Table 1, when the analysis indicates an inability of the System to meet the performance requirements in Table 1, the Planning Assessment shall include Corrective Action Plan(s) addressing how the performance requirements will be met. Revisions to the Corrective Action Plan(s) are allowed in subsequent Planning Assessments but the planned System shall continue to meet the performance requirements in Table 1. Corrective Action Plan(s) do not need to be developed solely to meet the performance requirements for a single sensitivity case analyzed in accordance with Requirements R2, Parts 2.1.4 and 2.4.3. The Corrective Action Plan(s) shall:
- 2.7.1. List System deficiencies and the associated actions needed to achieve required System performance. Examples of such actions include:
- Installation, modification, retirement, or removal of Transmission and generation Facilities and any associated equipment.
 - Installation, modification, or removal of Protection Systems or Special Protection Systems
 - Installation or modification of automatic generation tripping as a response to a single or multiple Contingency to mitigate Stability performance violations.
 - Installation or modification of manual and automatic generation runback/tripping as a response to a single or multiple Contingency to mitigate steady state performance violations.
 - Use of Operating Procedures specifying how long they will be needed as part of the Corrective Action Plan.
 - Use of rate applications, DSM, new technologies, or other initiatives.
- 2.7.2. Include actions to resolve performance deficiencies identified in multiple sensitivity studies or provide a rationale for why actions were not necessary.
- 2.7.3. If situations arise that are beyond the control of the Transmission Planner or Planning Coordinator that prevent the implementation of a Corrective Action Plan in the required timeframe, then the Transmission Planner or Planning Coordinator is permitted to utilize Non-Consequential Load Loss and curtailment of Firm Transmission Service to correct the situation that would normally not be permitted in Table 1, provided that the Transmission Planner

or Planning Coordinator documents that they are taking actions to resolve the situation. The Transmission Planner or Planning Coordinator shall document the situation causing the problem, alternatives evaluated, and the use of Non-Consequential Load Loss or curtailment of Firm Transmission Service.

- 2.7.4. Be reviewed in subsequent annual Planning Assessments for continued validity and implementation status of identified System Facilities and Operating Procedures.
- 2.8.** For short circuit analysis, if the short circuit current interrupting duty on circuit breakers determined in Requirement R2, Part 2.3 exceeds their Equipment Rating, the Planning Assessment shall include a Corrective Action Plan to address the Equipment Rating violations. The Corrective Action Plan shall:
 - 2.8.1. List System deficiencies and the associated actions needed to achieve required System performance.
 - 2.8.2. Be reviewed in subsequent annual Planning Assessments for continued validity and implementation status of identified System Facilities and Operating Procedures.
- R3.** For the steady state portion of the Planning Assessment, each Transmission Planner and Planning Coordinator shall perform studies for the Near-Term and Long-Term Transmission Planning Horizons in Requirement R2, Parts 2.1, and 2.2. The studies shall be based on computer simulation models using data provided in Requirement R1. [*Violation Risk Factor: Medium*] [*Time Horizon: Long-term Planning*]
 - 3.1.** Studies shall be performed for planning events to determine whether the BES meets the performance requirements in Table 1 based on the Contingency list created in Requirement R3, Part 3.4.
 - 3.2.** Studies shall be performed to assess the impact of the extreme events which are identified by the list created in Requirement R3, Part 3.5.
 - 3.3.** Contingency analyses for Requirement R3, Parts 3.1 & 3.2 shall:
 - 3.3.1. Simulate the removal of all elements that the Protection System and other automatic controls are expected to disconnect for each Contingency without operator intervention. The analyses shall include the impact of subsequent:
 - 3.3.1.1.** Tripping of generators where simulations show generator bus voltages or high side of the generation step up (GSU) voltages are less than known or assumed minimum generator steady state or ride through voltage limitations. Include in the assessment any assumptions made.
 - 3.3.1.2.** Tripping of Transmission elements where relay loadability limits are exceeded.
 - 3.3.2. Simulate the expected automatic operation of existing and planned devices designed to provide steady state control of electrical system quantities when such devices impact the study area. These devices may include equipment such as phase-shifting transformers, load tap changing transformers, and switched capacitors and inductors.
 - 3.4.** Those planning events in Table 1, that are expected to produce more severe System impacts on its portion of the BES, shall be identified and a list of those Contingencies

to be evaluated for System performance in Requirement R3, Part 3.1 created. The rationale for those Contingencies selected for evaluation shall be available as supporting information.

- 3.4.1. The Planning Coordinator and Transmission Planner shall coordinate with adjacent Planning Coordinators and Transmission Planners to ensure that Contingencies on adjacent Systems which may impact their Systems are included in the Contingency list.
- 3.5. Those extreme events in Table 1 that are expected to produce more severe System impacts shall be identified and a list created of those events to be evaluated in Requirement R3, Part 3.2. The rationale for those Contingencies selected for evaluation shall be available as supporting information. If the analysis concludes there is Cascading caused by the occurrence of extreme events, an evaluation of possible actions designed to reduce the likelihood or mitigate the consequences and adverse impacts of the event(s) shall be conducted.
- R4.** For the Stability portion of the Planning Assessment, as described in Requirement R2, Parts 2.4 and 2.5, each Transmission Planner and Planning Coordinator shall perform the Contingency analyses listed in Table 1. The studies shall be based on computer simulation models using data provided in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*
 - 4.1. Studies shall be performed for planning events to determine whether the BES meets the performance requirements in Table 1 based on the Contingency list created in Requirement R4, Part 4.4.
 - 4.1.1. For planning event P1: No generating unit shall pull out of synchronism. A generator being disconnected from the System by fault clearing action or by a Special Protection System is not considered pulling out of synchronism.
 - 4.1.2. For planning events P2 through P7: When a generator pulls out of synchronism in the simulations, the resulting apparent impedance swings shall not result in the tripping of any Transmission system elements other than the generating unit and its directly connected Facilities.
 - 4.1.3. For planning events P1 through P7: Power oscillations shall exhibit acceptable damping as established by the Planning Coordinator and Transmission Planner.
 - 4.2. Studies shall be performed to assess the impact of the extreme events which are identified by the list created in Requirement R4, Part 4.5.
 - 4.3. Contingency analyses for Requirement R4, Parts 4.1 and 4.2 shall :
 - 4.3.1. Simulate the removal of all elements that the Protection System and other automatic controls are expected to disconnect for each Contingency without operator intervention. The analyses shall include the impact of subsequent:
 - 4.3.1.1. Successful high speed (less than one second) reclosing and unsuccessful high speed reclosing into a Fault where high speed reclosing is utilized.
 - 4.3.1.2. Tripping of generators where simulations show generator bus voltages or high side of the GSU voltages are less than known or assumed generator low voltage ride through capability. Include in the assessment any assumptions made.

Table 1 – Steady State & Stability Performance Planning Events

Steady State & Stability:

- a. The System shall remain stable. Cascading and uncontrolled islanding shall not occur.
- b. Consequential Load Loss as well as generation loss is acceptable as a consequence of any event excluding P0.
- c. Simulate the removal of all elements that Protection Systems and other controls are expected to automatically disconnect for each event.
- d. Simulate Normal Clearing unless otherwise specified.
- e. Planned System adjustments such as Transmission configuration changes and re-dispatch of generation are allowed if such adjustments are executable within the time duration applicable to the Facility Ratings.

Steady State Only:

- f. Applicable Facility Ratings shall not be exceeded.
- g. System steady state voltages and post-Contingency voltage deviations shall be within acceptable limits as established by the Planning Coordinator and the Transmission Planner.
- h. Planning event P0 is applicable to steady state only.
- i. The response of voltage sensitive Load that is disconnected from the System by end-user equipment associated with an event shall not be used to meet steady state performance requirements.

Stability Only:

- j. Transient voltage response shall be within acceptable limits established by the Planning Coordinator and the Transmission Planner.

Category	Initial Condition	Event ¹	Fault Type ²	BES Level ³	Interruption of Firm Transmission Service Allowed ⁴	Non-Consequential Load Loss Allowed
P0 No Contingency	Normal System	None	N/A	EHV, HV	No	No
P1 Single Contingency	Normal System	Loss of one of the following: 1. Generator 2. Transmission Circuit 3. Transformer ⁵ 4. Shunt Device ⁶	3Ø	EHV, HV	No ⁹	No ¹²
		5. Single Pole of a DC line	SLG			
P2 Single Contingency	Normal System	1. Opening of a line section w/o a fault ⁷	N/A	EHV, HV	No ⁹	No ¹²
		2. Bus Section Fault	SLG	EHV	No ⁹	No
				HV	Yes	Yes
		3. Internal Breaker Fault ⁸ (non-Bus-tie Breaker)	SLG	EHV	No ⁹	No
HV	Yes			Yes		
4. Internal Breaker Fault (Bus-tie Breaker) ⁸	SLG	EHV, HV	Yes	Yes		

Standard TPL-001-4 — Transmission System Planning Performance Requirements

Category	Initial Condition	Event ¹	Fault Type ²	BES Level ³	Interruption of Firm Transmission Service Allowed ⁴	Non-Consequential Load Loss Allowed
P3 Multiple Contingency	Loss of generator unit followed by System adjustments ⁹	Loss of one of the following: 1. Generator 2. Transmission Circuit 3. Transformer ⁵ 4. Shunt Device ⁶	3Ø	EHV, HV	No ⁹	No ¹²
		5. Single pole of a DC line	SLG			
P4 Multiple Contingency <i>(Fault plus stuck breaker¹⁰)</i>	Normal System	Loss of multiple elements caused by a stuck breaker ¹⁰ (non-Bus-tie Breaker) attempting to clear a Fault on one of the following: 1. Generator 2. Transmission Circuit 3. Transformer ⁵ 4. Shunt Device ⁶ 5. Bus Section	SLG	EHV	No ⁹	No
		6. Loss of multiple elements caused by a stuck breaker ¹⁰ (Bus-tie Breaker) attempting to clear a Fault on the associated bus		HV	Yes	Yes
				SLG	EHV, HV	Yes
P5 Multiple Contingency <i>(Fault plus relay failure to operate)</i>	Normal System	Delayed Fault Clearing due to the failure of a non-redundant relay ¹³ protecting the Faulted element to operate as designed, for one of the following: 1. Generator 2. Transmission Circuit 3. Transformer ⁵ 4. Shunt Device ⁶ 5. Bus Section	SLG	EHV	No ⁹	No
				HV	Yes	Yes
P6 Multiple Contingency <i>(Two overlapping singles)</i>	Loss of one of the following followed by System adjustments. ⁹ 1. Transmission Circuit 2. Transformer ⁵ 3. Shunt Device ⁶ 4. Single pole of a DC line	Loss of one of the following: 1. Transmission Circuit 2. Transformer ⁵ 3. Shunt Device ⁶	3Ø	EHV, HV	Yes	Yes
		4. Single pole of a DC line	SLG			

Standard TPL-001-4 — Transmission System Planning Performance Requirements

Category	Initial Condition	Event ¹	Fault Type ²	BES Level ³	Interruption of Firm Transmission Service Allowed ⁴	Non-Consequential Load Loss Allowed
P7 Multiple Contingency <i>(Common Structure)</i>	Normal System	The loss of: 1. Any two adjacent (vertically or horizontally) circuits on common structure ¹¹ 2. Loss of a bipolar DC line	SLG	EHV, HV	Yes	Yes

Table 1 – Steady State & Stability Performance Extreme Events

Steady State & Stability

For all extreme events evaluated:

- a. Simulate the removal of all elements that Protection Systems and automatic controls are expected to disconnect for each Contingency.
- b. Simulate Normal Clearing unless otherwise specified.

Steady State

1. Loss of a single generator, Transmission Circuit, single pole of a DC Line, shunt device, or transformer forced out of service followed by another single generator, Transmission Circuit, single pole of a different DC Line, shunt device, or transformer forced out of service prior to System adjustments.
2. Local area events affecting the Transmission System such as:
 - a. Loss of a tower line with three or more circuits.¹¹
 - b. Loss of all Transmission lines on a common Right-of-Way¹¹.
 - c. Loss of a switching station or substation (loss of one voltage level plus transformers).
 - d. Loss of all generating units at a generating station.
 - e. Loss of a large Load or major Load center.
3. Wide area events affecting the Transmission System based on System topology such as:
 - a. Loss of two generating stations resulting from conditions such as:
 - i. Loss of a large gas pipeline into a region or multiple regions that have significant gas-fired generation.
 - ii. Loss of the use of a large body of water as the cooling source for generation.
 - iii. Wildfires.
 - iv. Severe weather, e.g., hurricanes, tornadoes, etc.
 - v. A successful cyber attack.
 - vi. Shutdown of a nuclear power plant(s) and related facilities for a day or more for common causes such as problems with similarly designed plants.
 - b. Other events based upon operating experience that may result in wide area disturbances.

Stability

1. With an initial condition of a single generator, Transmission circuit, single pole of a DC line, shunt device, or transformer forced out of service, apply a 3Ø fault on another single generator, Transmission circuit, single pole of a different DC line, shunt device, or transformer prior to System adjustments.
2. Local or wide area events affecting the Transmission System such as:
 - a. 3Ø fault on generator with stuck breaker¹⁰ or a relay failure¹³ resulting in Delayed Fault Clearing.
 - b. 3Ø fault on Transmission circuit with stuck breaker¹⁰ or a relay failure¹³ resulting in Delayed Fault Clearing.
 - c. 3Ø fault on transformer with stuck breaker¹⁰ or a relay failure¹³ resulting in Delayed Fault Clearing.
 - d. 3Ø fault on bus section with stuck breaker¹⁰ or a relay failure¹³ resulting in Delayed Fault Clearing.
 - e. 3Ø internal breaker fault.
 - f. Other events based upon operating experience, such as consideration of initiating events that experience suggests may result in wide area disturbances

**Table 1 – Steady State & Stability Performance Footnotes
(Planning Events and Extreme Events)**

1. If the event analyzed involves BES elements at multiple System voltage levels, the lowest System voltage level of the element(s) removed for the analyzed event determines the stated performance criteria regarding allowances for interruptions of Firm Transmission Service and Non-Consequential Load Loss.
2. Unless specified otherwise, simulate Normal Clearing of faults. Single line to ground (SLG) or three-phase (3Ø) are the fault types that must be evaluated in Stability simulations for the event described. A 3Ø or a double line to ground fault study indicating the criteria are being met is sufficient evidence that a SLG condition would also meet the criteria.
3. Bulk Electric System (BES) level references include extra-high voltage (EHV) Facilities defined as greater than 300kV and high voltage (HV) Facilities defined as the 300kV and lower voltage Systems. The designation of EHV and HV is used to distinguish between stated performance criteria allowances for interruption of Firm Transmission Service and Non-Consequential Load Loss.
4. Curtailment of Conditional Firm Transmission Service is allowed when the conditions and/or events being studied formed the basis for the Conditional Firm Transmission Service.
5. For non-generator step up transformer outage events, the reference voltage, as used in footnote 1, applies to the low-side winding (excluding tertiary windings). For generator and Generator Step Up transformer outage events, the reference voltage applies to the BES connected voltage (high-side of the Generator Step Up transformer). Requirements which are applicable to transformers also apply to variable frequency transformers and phase shifting transformers.
6. Requirements which are applicable to shunt devices also apply to FACTS devices that are connected to ground.
7. Opening one end of a line section without a fault on a normally networked Transmission circuit such that the line is possibly serving Load radial from a single source point.
8. An internal breaker fault means a breaker failing internally, thus creating a System fault which must be cleared by protection on both sides of the breaker.
9. An objective of the planning process should be to minimize the likelihood and magnitude of interruption of Firm Transmission Service following Contingency events. Curtailment of Firm Transmission Service is allowed both as a System adjustment (as identified in the column entitled 'Initial Condition') and a corrective action when achieved through the appropriate re-dispatch of resources obligated to re-dispatch, where it can be demonstrated that Facilities, internal and external to the Transmission Planner's planning region, remain within applicable Facility Ratings and the re-dispatch does not result in any Non-Consequential Load Loss. Where limited options for re-dispatch exist, sensitivities associated with the availability of those resources should be considered.
10. A stuck breaker means that for a gang-operated breaker, all three phases of the breaker have remained closed. For an independent pole operated (IPO) or an independent pole tripping (IPT) breaker, only one pole is assumed to remain closed. A stuck breaker results in Delayed Fault Clearing.
11. Excludes circuits that share a common structure (Planning event P7, Extreme event steady state 2a) or common Right-of-Way (Extreme event, steady state 2b) for 1 mile or less.
12. An objective of the planning process is to minimize the likelihood and magnitude of Non-Consequential Load Loss following planning events. In limited circumstances, Non-Consequential Load Loss may be needed throughout the planning horizon to ensure that BES performance requirements are met. However, when Non-Consequential Load Loss is utilized under footnote 12 within the Near-Term Transmission Planning Horizon to address BES performance requirements, such interruption is limited to circumstances where the Non-Consequential Load Loss meets the conditions shown in Attachment 1. In no case can the planned Non-Consequential Load Loss under footnote 12 exceed 75 MW for US registered entities. The amount of planned Non-Consequential Load Loss for a non-US Registered Entity should be implemented in a manner that is consistent with, or under the direction of, the applicable governmental authority or its agency in the non-US jurisdiction.
13. Applies to the following relay functions or types: pilot (#85), distance (#21), differential (#87), current (#50, 51, and 67), voltage (#27 & 59), directional (#32, &

**Table 1 – Steady State & Stability Performance Footnotes
(Planning Events and Extreme Events)**

67), and tripping (#86, & 94).

Attachment 1

I. Stakeholder Process

During each Planning Assessment before the use of Non-Consequential Load Loss under footnote 12 is allowed as an element of a Corrective Action Plan in the Near-Term Transmission Planning Horizon of the Planning Assessment, the Transmission Planner or Planning Coordinator shall ensure that the utilization of footnote 12 is reviewed through an open and transparent stakeholder process. The responsible entity can utilize an existing process or develop a new process. The process must include the following:

1. Meetings must be open to affected stakeholders including applicable regulatory authorities or governing bodies responsible for retail electric service issues
2. Notice must be provided in advance of meetings to affected stakeholders including applicable regulatory authorities or governing bodies responsible for retail electric service issues and include an agenda with:
 - a. Date, time, and location for the meeting
 - b. Specific location(s) of the planned Non-Consequential Load Loss under footnote 12
 - c. Provisions for a stakeholder comment period
3. Information regarding the intended purpose and scope of the proposed Non-Consequential Load Loss under footnote 12 (as shown in Section II below) must be made available to meeting participants
4. A procedure for stakeholders to submit written questions or concerns and to receive written responses to the submitted questions and concerns
5. A dispute resolution process for any question or concern raised in #4 above that is not resolved to the stakeholder's satisfaction

An entity does not have to repeat the stakeholder process for a specific application of footnote 12 utilization with respect to subsequent Planning Assessments unless conditions spelled out in Section II below have materially changed for that specific application.

II. Information for Inclusion in Item #3 of the Stakeholder Process

The responsible entity shall document the planned use of Non-Consequential Load Loss under footnote 12 which must include the following:

1. Conditions under which Non-Consequential Load Loss under footnote 12 would be necessary:
 - a. System Load level and estimated annual hours of exposure at or above that Load level
 - b. Applicable Contingencies and the Facilities outside their applicable rating due to that Contingency
2. Amount of Non-Consequential Load Loss with:
 - a. The estimated number and type of customers affected

Standard TPL-001-4 — Transmission System Planning Performance Requirements

- b. An explanation of the effect of the use of Non-Consequential Load Loss under footnote 12 on the health, safety, and welfare of the community
3. Estimated frequency of Non-Consequential Load Loss under footnote 12 based on historical performance
4. Expected duration of Non-Consequential Load Loss under footnote 12 based on historical performance
5. Future plans to alleviate the need for Non-Consequential Load Loss under footnote 12
6. Verification that TPL Reliability Standards performance requirements will be met following the application of footnote 12
7. Alternatives to Non-Consequential Load Loss considered and the rationale for not selecting those alternatives under footnote 12
8. Assessment of potential overlapping uses of footnote 12 including overlaps with adjacent Transmission Planners and Planning Coordinators

III. Instances for which Regulatory Review of Non-Consequential Load Loss under Footnote 12 is Required

Before a Non-Consequential Load Loss under footnote 12 is allowed as an element of a Corrective Action Plan in Year One of the Planning Assessment, the Transmission Planner or Planning Coordinator must ensure that the applicable regulatory authorities or governing bodies responsible for retail electric service issues do not object to the use of Non-Consequential Load Loss under footnote 12 if either:

1. The voltage level of the Contingency is greater than 300 kV
 - a. If the Contingency analyzed involves BES Elements at multiple System voltage levels, the lowest System voltage level of the element(s) removed for the analyzed Contingency determines the stated performance criteria regarding allowances for Non-Consequential Load Loss under footnote 12, or
 - b. For a non-generator step up transformer outage Contingency, the 300 kV limit applies to the low-side winding (excluding tertiary windings). For a generator or generator step up transformer outage Contingency, the 300 kV limit applies to the BES connected voltage (high-side of the Generator Step Up transformer)
2. The planned Non-Consequential Load Loss under footnote 12 is greater than or equal to 25 MW

Once assurance has been received that the applicable regulatory authorities or governing bodies responsible for retail electric service issues do not object to the use of Non-Consequential Load Loss under footnote 12, the Planning Coordinator or Transmission Planner must submit the information outlined in items II.1 through II.8 above to the ERO for a determination of whether there are any Adverse Reliability Impacts caused by the request to utilize footnote 12 for Non-Consequential Load Loss.

C. Measures

- M1.** Each Transmission Planner and Planning Coordinator shall provide evidence, in electronic or hard copy format, that it is maintaining System models within their respective area, using data consistent with MOD-010 and MOD-012, including items represented in the Corrective Action Plan, representing projected System conditions, and that the models represent the required information in accordance with Requirement R1.
- M2.** Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of its annual Planning Assessment, that it has prepared an annual Planning Assessment of its portion of the BES in accordance with Requirement R2.
- M3.** Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of the studies utilized in preparing the Planning Assessment, in accordance with Requirement R3.
- M4.** Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of the studies utilized in preparing the Planning Assessment in accordance with Requirement R4.
- M5.** Each Transmission Planner and Planning Coordinator shall provide dated evidence such as electronic or hard copies of the documentation specifying the criteria for acceptable System steady state voltage limits, post-Contingency voltage deviations, and the transient voltage response for its System in accordance with Requirement R5.
- M6.** Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of documentation specifying the criteria or methodology used in the analysis to identify System instability for conditions such as Cascading, voltage instability, or uncontrolled islanding that was utilized in preparing the Planning Assessment in accordance with Requirement R6.
- M7.** Each Planning Coordinator, in conjunction with each of its Transmission Planners, shall provide dated documentation on roles and responsibilities, such as meeting minutes, agreements, and e-mail correspondence that identifies that agreement has been reached on individual and joint responsibilities for performing the required studies and Assessments in accordance with Requirement R7.
- M8.** Each Planning Coordinator and Transmission Planner shall provide evidence, such as email notices, documentation of updated web pages, postal receipts showing recipient and date; or a demonstration of a public posting, that it has distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners within 90 days of having completed its Planning Assessment, and to any functional entity who has indicated a reliability need within 30 days of a written request and that the Planning Coordinator or Transmission Planner has provided a documented response to comments received on Planning Assessment results within 90 calendar days of receipt of those comments in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

Regional Entity

1.2 Compliance Monitoring Period and Reset Timeframe

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

The Transmission Planner and Planning Coordinator shall each retain data or evidence to show compliance as identified unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The models utilized in the current in-force Planning Assessment and one previous Planning Assessment in accordance with Requirement R1 and Measure M1.
- The Planning Assessments performed since the last compliance audit in accordance with Requirement R2 and Measure M2.
- The studies performed in support of its Planning Assessments since the last compliance audit in accordance with Requirement R3 and Measure M3.
- The studies performed in support of its Planning Assessments since the last compliance audit in accordance with Requirement R4 and Measure M4.
- The documentation specifying the criteria for acceptable System steady state voltage limits, post-Contingency voltage deviations, and transient voltage response since the last compliance audit in accordance with Requirement R5 and Measure M5.
- The documentation specifying the criteria or methodology utilized in the analysis to identify System instability for conditions such as Cascading, voltage instability, or uncontrolled islanding in support of its Planning Assessments since the last compliance audit in accordance with Requirement R6 and Measure M6.
- The current, in force documentation for the agreement(s) on roles and responsibilities, as well as documentation for the agreements in force since the last compliance audit, in accordance with Requirement R7 and Measure M7.

The Planning Coordinator shall retain data or evidence to show compliance as identified unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Three calendar years of the notifications employed in accordance with Requirement R8 and Measure M8.

If a Transmission Planner or Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or the time periods specified above, whichever is longer.

1.5 Additional Compliance Information

None

2. Violation Severity Levels

	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's System model failed to represent one of the Requirement R1, Parts 1.1.1 through 1.1.6.	The responsible entity's System model failed to represent two of the Requirement R1, Parts 1.1.1 through 1.1.6.	The responsible entity's System model failed to represent three of the Requirement R1, Parts 1.1.1 through 1.1.6.	The responsible entity's System model failed to represent four or more of the Requirement R1, Parts 1.1.1 through 1.1.6. OR The responsible entity's System model did not represent projected System conditions as described in Requirement R1. OR The responsible entity's System model did not use data consistent with that provided in accordance with the MOD-010 and MOD-012 standards and other sources, including items represented in the Corrective Action Plan.
R2	The responsible entity failed to comply with Requirement R2, Part 2.6.	The responsible entity failed to comply with Requirement R2, Part 2.3 or Part 2.8.	The responsible entity failed to comply with one of the following Parts of Requirement R2: Part 2.1, Part 2.2, Part 2.4, Part 2.5, or Part 2.7.	The responsible entity failed to comply with two or more of the following Parts of Requirement R2: Part 2.1, Part 2.2, Part 2.4, or Part 2.7. OR The responsible entity does not have a completed annual Planning Assessment.
R3	The responsible entity did not identify planning events as described in Requirement R3, Part 3.4 or extreme events as described in Requirement R3, Part 3.5.	The responsible entity did not perform studies as specified in Requirement R3, Part 3.1 to determine that the BES meets the performance requirements for one of the categories (P2 through P7) in Table 1.	The responsible entity did not perform studies as specified in Requirement R3, Part 3.1 to determine that the BES meets the performance requirements for two of the categories (P2 through P7) in	The responsible entity did not perform studies as specified in Requirement R3, Part 3.1 to determine that the BES meets the performance requirements for three or more of the categories (P2 through P7) in Table 1.

Standard TPL-001-4 — Transmission System Planning Performance Requirements

	Lower VSL	Moderate VSL	High VSL	Severe VSL
		<p>OR</p> <p>The responsible entity did not perform studies as specified in Requirement R3, Part 3.2 to assess the impact of extreme events.</p>	<p>Table 1.</p> <p>OR</p> <p>The responsible entity did not perform Contingency analysis as described in Requirement R3, Part 3.3.</p>	<p>OR</p> <p>The responsible entity did not perform studies to determine that the BES meets the performance requirements for the P0 or P1 categories in Table 1.</p> <p>OR</p> <p>The responsible entity did not base its studies on computer simulation models using data provided in Requirement R1.</p>
R4	<p>The responsible entity did not identify planning events as described in Requirement R4, Part 4.4 or extreme events as described in Requirement R4, Part 4.5.</p>	<p>The responsible entity did not perform studies as specified in Requirement R4, Part 4.1 to determine that the BES meets the performance requirements for one of the categories (P1 through P7) in Table 1.</p> <p>OR</p> <p>The responsible entity did not perform studies as specified in Requirement R4, Part 4.2 to assess the impact of extreme events.</p>	<p>The responsible entity did not perform studies as specified in Requirement R4, Part 4.1 to determine that the BES meets the performance requirements for two of the categories (P1 through P7) in Table 1.</p> <p>OR</p> <p>The responsible entity did not perform Contingency analysis as described in Requirement R4, Part 4.3.</p>	<p>The responsible entity did not perform studies as specified in Requirement R4, Part 4.1 to determine that the BES meets the performance requirements for three or more of the categories (P1 through P7) in Table 1.</p> <p>OR</p> <p>The responsible entity did not base its studies on computer simulation models using data provided in Requirement R1.</p>
R5	N/A	N/A	N/A	<p>The responsible entity does not have criteria for acceptable System steady state voltage limits, post-Contingency voltage deviations, or the transient voltage response for its System.</p>
R6	N/A	N/A	N/A	<p>The responsible entity failed to define and document the criteria or methodology for System instability used within its analysis as described in Requirement R6.</p>

Standard TPL-001-4 — Transmission System Planning Performance Requirements

	Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	N/A	N/A	N/A	The Planning Coordinator, in conjunction with each of its Transmission Planners, failed to determine and identify individual or joint responsibilities for performing required studies.
R8	<p>The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 90 days but less than or equal to 120 days following its completion.</p> <p>OR,</p> <p>The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 30 days but less than or equal to 40 days following the request.</p>	<p>The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 120 days but less than or equal to 130 days following its completion.</p> <p>OR,</p> <p>The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 40 days but less than or equal to 50 days following the request.</p>	<p>The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 130 days but less than or equal to 140 days following its completion.</p> <p>OR,</p> <p>The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 50 days but less than or equal to 60 days following the request.</p>	<p>The responsible entity distributed its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners but it was more than 140 days following its completion.</p> <p>OR</p> <p>The responsible entity did not distribute its Planning Assessment results to adjacent Planning Coordinators and adjacent Transmission Planners.</p> <p>OR</p> <p>The responsible entity distributed its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing but it was more than 60 days following the request.</p> <p>OR</p> <p>The responsible entity did not distribute its Planning Assessment results to functional entities having a reliability related need who requested the Planning Assessment in writing.</p>

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	February 8, 2005	BOT Approval	Revised
0	June 3, 2005	Fixed reference in M1 to read TPL-001-0 R2.1 and TPL-001-0 R2.2	Errata
0	July 24, 2007	Corrected reference in M1. to read TPL-001-0 R1 and TPL-001-0 R2.	Errata
0.1	October 29, 2008	BOT adopted errata changes; updated version number to "0.1"	Errata
0.1	May 13, 2009	FERC Approved – Updated Effective Date and Footer	Revised
1	Approved by Board of Trustees February 17, 2011	Revised footnote 'b' pursuant to FERC Order RM06-16-009	Revised (Project 2010-11)
2	August 4, 2011	Revision of TPL-001-1; includes merging and upgrading requirements of TPL-001-0, TPL-002-0, TPL-003-0, and TPL-004-0 into one, single, comprehensive, coordinated standard: TPL-001-2; and retirement of TPL-005-0 and TPL-006-0.	Project 2006-02 – complete revision
2	August 4, 2011	Adopted by Board of Trustees	
1	April 19, 2012	FERC issued Order 762 remanding TPL-001-1, TPL-002-1b, TPL-003-1a, and TPL-004-1. FERC also issued a NOPR proposing to remand TPL-001-2. NERC has been directed to revise footnote 'b' in accordance with the directives of Order Nos. 762 and 693.	
3	February 7, 2013	Adopted by the NERC Board of Trustees. TPL-001-3 was created after the Board of Trustees approved the revised footnote 'b' in TPL-002-2b, which was balloted and appended to: TPL-001-0.1, TPL-002-0b, TPL-003-0a, and TPL-004-0.	
4	February 7, 2013	Adopted by the NERC Board of Trustees. TPL-001-4 was adopted by the Board of Trustees as TPL-001-3, but a discrepancy in numbering was identified and corrected prior to filing with the regulatory agencies.	
4	October 17, 2013	FERC Order issued approving TPL-001-4 (Order effective December 23, 2013).	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard TPL-001-4 — Transmission System Planning Performance Requirements

United States

Standard	Requirement	Enforcement Date	Inactive Date
TPL-001-4	R1.	01/01/2015	
TPL-001-4	R2.	01/01/2016	
TPL-001-4	R3.	01/01/2016	
TPL-001-4	R4.	01/01/2016	
TPL-001-4	R5.	01/01/2016	
TPL-001-4	R6.	01/01/2016	
TPL-001-4	R7.	01/01/2015	
TPL-001-4	R8.	01/01/2016	

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization
2. **Number:** CIP-002-5.1
3. **Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**
 - 4.1.4. **Generator Owner**

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1:

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

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

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

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

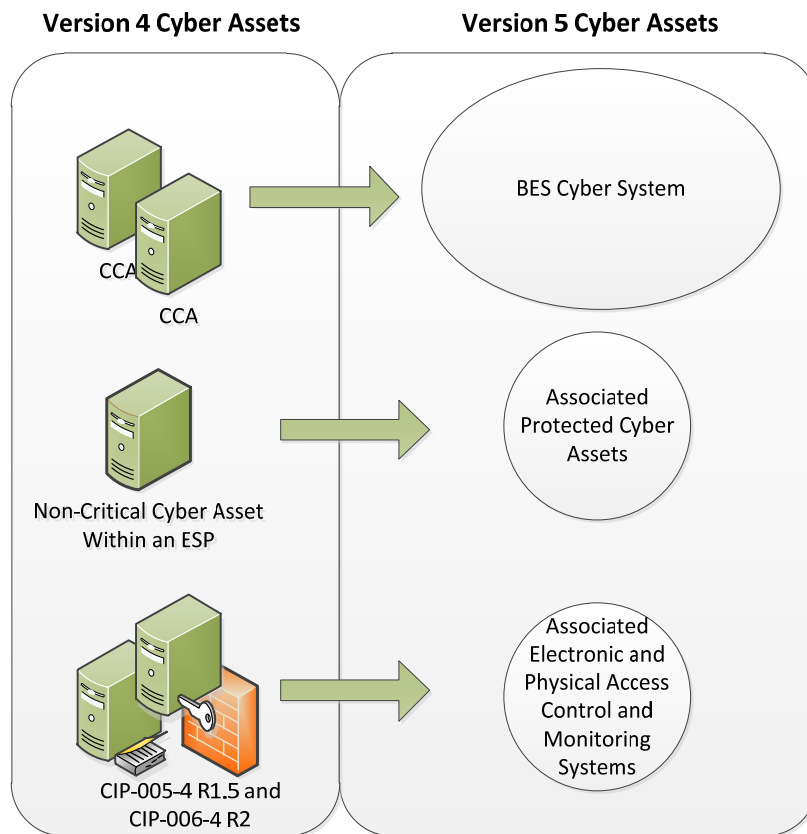
This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

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



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

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

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

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

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems (“EACMS”) – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems (“PACS”)– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets (“PCA”) – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [*Violation Risk Factor: High*][*Time Horizon: Operations Planning*]
- i.** Control Centers and backup Control Centers;
 - ii.** Transmission stations and substations;
 - iii.** Generation resources;
 - iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
 - v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
 - vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
- 1.1.** Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;
 - 1.2.** Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and
 - 1.3.** Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).
- M1.** Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- 2.1** Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and
- 2.2** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	High	<p>For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1;</p> <p>OR</p> <p>For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1;</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BES Cyber</p>	<p>For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1;</p> <p>OR</p> <p>For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1;</p> <p>OR</p> <p>For Responsible</p>	<p>For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1;</p> <p>OR</p> <p>For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1;</p> <p>OR</p> <p>For Responsible</p>	<p>For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1;</p> <p>OR</p> <p>For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1;</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BES Cyber</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BES Cyber</p>	<p>Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower</p>	<p>Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower</p>	<p>Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BES Cyber</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>Systems, five percent or fewer high or medium BES Cyber Systems have not been identified;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.</p>	<p>category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.</p>	<p>category.</p> <p>OR</p> <p>For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.</p>	<p>Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified;</p> <p>OR</p> <p>For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	Lower	<p>The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)</p>	<p>The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1)</p> <p>OR</p> <p>The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)</p>	<p>The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1)</p> <p>OR</p> <p>The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)</p>	<p>The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1)</p> <p>OR</p> <p>The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)</p>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5.1 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

- 1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
- 1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
- 1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
- 1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
- 2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

- 2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
- 2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
- 2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

- 2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.
- 2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

- 2.10.** Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.
- 2.11.** Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.
- 2.12.** Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.
- 2.13.** Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

- 3.1.** Control Centers and backup Control Centers.
- 3.2.** Transmission stations and substations.
- 3.3.** Generation resources.
- 3.4.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.
- 3.5.** Special Protection Systems that support the reliable operation of the Bulk Electric System.
- 3.6.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1

CIP-002-5.1 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “...that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5.1. The concept includes a number of named BES reliability operating services. These named services include:

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

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

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

Dynamic Response

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

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

Balancing Load and Generation

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

- Calculation of Area Control Error (ACE)
 - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
 - Software used to perform calculation (BA)
- Demand Response
 - Ability to identify load change need (BA)
 - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
 - Ability to identify load change need (BA)
 - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
 - Know generation status, capability, ramp rate, start time (GO, BA)
 - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

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

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

Controlling Voltage (Reactive Power)

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

- Automatic Voltage Regulation (AVR)
 - Sensors, stator control system, feedback (GO)
- Capacitive resources
 - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
 - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
 - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

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

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

Monitoring and Control

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

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

Restoration of BES

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

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

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

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

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

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

Applicability to Distribution Providers

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

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term “Facilities”, there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

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

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

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

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

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.
- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.
- Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.
- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the “Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface.” This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:
 - Excluded radial facilities that would only provide support for single generation facilities.
 - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

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

Additionally, in NERC’s document “[Integrated Risk Assessment Approach – Refinement to Severity Risk Index](#)”, Attachment 1, the report used an average MVA line loading based on kV rating:

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

In the terms of applicable lines and connecting “other Transmission stations or substations” determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the “fence” of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5’s qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

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

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.
- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.
- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.
- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource (“LaaR”) Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.
- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

In response, the CIP Version 5 drafting team sought informal input from NERC’s Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

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

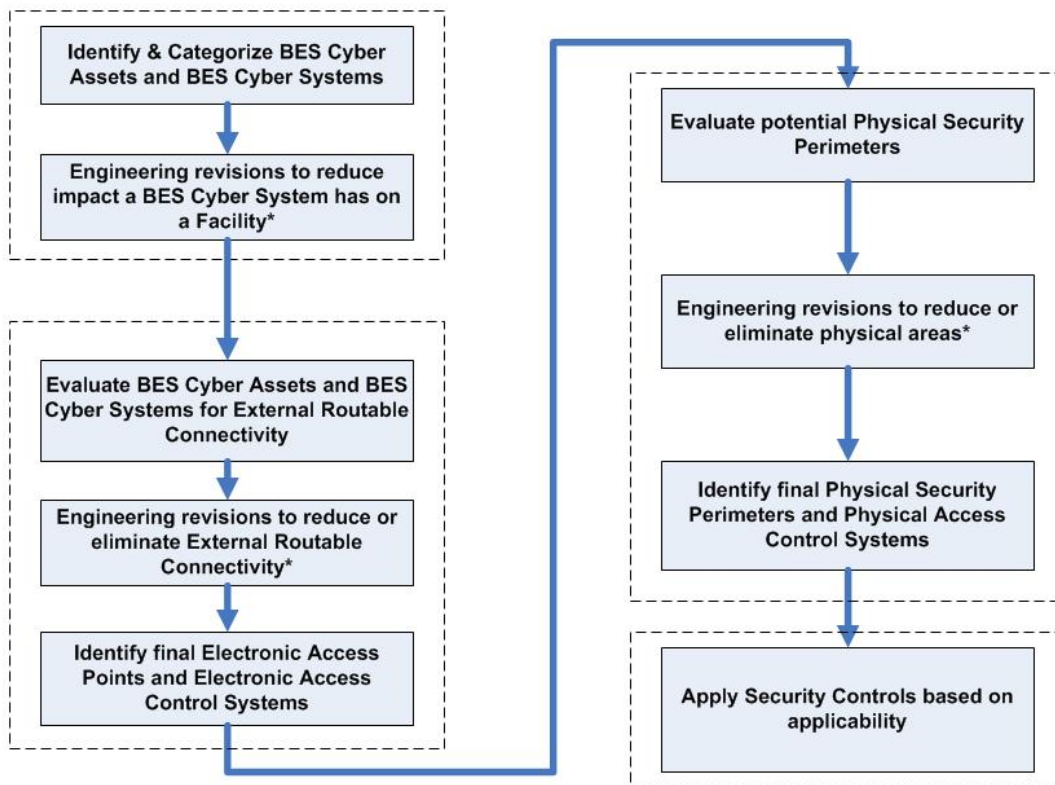
- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

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

Overview (Generation Facility)



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

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of “bright-line” criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3.	Update

Guidelines and Technical Basis

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced "Devices" with "Systems" in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-002-5.1 — Cyber Security — BES Cyber System Categorization

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-002-5.1	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-5
3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**
 - 4.1.6 **Reliability Coordinator**

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

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

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies**, . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects

are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

- R1.** Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- 1.1** Personnel & training (CIP-004);
 - 1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
 - 1.3** Physical security of BES Cyber Systems (CIP-006);
 - 1.4** System security management (CIP-007);
 - 1.5** Incident reporting and response planning (CIP-008);
 - 1.6** Recovery plans for BES Cyber Systems (CIP-009);
 - 1.7** Configuration change management and vulnerability assessments (CIP-010);
 - 1.8** Information protection (CIP-011); and
 - 1.9** Declaring and responding to CIP Exceptional Circumstances.
- M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.
- R2.** Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- 2.1** Cyber security awareness;
 - 2.2** Physical security controls;
 - 2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
 - 2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

- M2.** Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

- R3.** Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium]*
[Time Horizon: Operations Planning]

- M3.** An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

- R4.** The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower]* *[Time Horizon: Operations Planning]*

- M4.** An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1)</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1)</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1)</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1)</p> <p>OR</p> <p>The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1)</p> <p>OR</p> <p>The Responsible</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>in less than or equal to 16 calendar months of the previous review. (R1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous</p>	<p>in less than or equal to 17 calendar months of the previous review. (R1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous</p>	<p>previous review. (R1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)</p>	<p>Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval. (R1)	approval. (R1)		previous approval. (R1)
R2	Operations Planning	Lower	<p>The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2)</p> <p>OR</p> <p>The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2)</p> <p>OR</p> <p>The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as</p>	<p>The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2)</p> <p>OR</p> <p>The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies.</p>	<p>The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2)</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)</p> <p>OR</p> <p>The Responsible</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>required by R2 but did not identify, assess, or correct the deficiencies.</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one</p>	<p>required by R2 but did not identify, assess, or correct the deficiencies.</p> <p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one</p>	<p>OR</p> <p>The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2)</p> <p>OR</p> <p>The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 17 calendar months but</p>	<p>Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 18 calendar months of the previous approval. (R2)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	
R3	Operations Planning	Medium	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			40 calendar days of the change. (R3)	change in less than 50 calendar days of the change. (R3)	days of the change. (R3)	Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	Operations Planning	Lower	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

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

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

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

1.5 Incident reporting and response planning (CIP-008)

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

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

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

1.8 Information protection (CIP-011)

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

1.9 Declaring and responding to CIP Exceptional Circumstances

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

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

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

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term “electronic access control” in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

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

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

Rationale for R2:

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

The language in Requirement R2, Part 2.3 “. . . for external routable protocol connections and Dial-up Connectivity . . .” was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections “of some form” to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase “external routable protocol connections” instead of the defined term “External Routable Connectivity,” because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term “External Routable Connectivity” in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5. (Order becomes effective 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-003-5 — Cyber Security - Security Management Controls

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-003-5	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-5.1
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. Applicability:

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

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

- 4.1.2.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.1.2.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5.1:

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

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

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

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-004-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-004-5.1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, *“Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying “implement” as follows:

Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the “. . . identifies, assesses, and corrects deficiencies, . . .” elements described in the preceding paragraph, as those aspects are related to the manner of

implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5.1 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: <ul style="list-style-type: none"> • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

- R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program*. [*Violation Risk Factor: Lower*]
[*Time Horizon: Operations Planning*]
- M2.** Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Training content on:</p> <ol style="list-style-type: none"> 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets. 	<p>Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.</p>

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.</p>	<p>Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Require completion of the training specified in Part 2.1 at least once every 15 calendar months.</p>	<p>Examples of evidence may include, but are not limited to, dated individual training records.</p>

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R3 – Personnel Risk Assessment Program*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to confirm identity.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. <p>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to perform a seven year criminal history records check.</p>

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Criteria or process to evaluate criminal history records checks for authorizing access.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to evaluate criminal history records checks.</p>
3.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments.</p>

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.</p>

- R4.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R4 – Access Management Program*. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning and Same Day Operations*].
- M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5.1 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ol style="list-style-type: none"> 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. 	<p>An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.</p>

CIP-004-5.1 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-5.1 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.</p>	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-5.1 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.</p>	<p>An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

- R5.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.</p>	<p>An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.</p>

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> EACMS 	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.5	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p> <p>If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> Workflow or sign-off form showing password reset within 30 calendar days of the termination; Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized</p>	<p>deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical</p>	<p>deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical</p>	<p>implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies.</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion</p>	<p>access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)</p>	<p>access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)</p>	<p>(2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	Operations Planning	Medium	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including</p>	<p>The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3)</p> <p>OR</p> <p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access</p>	<p>calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)</p>	<p>calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)</p>	<p>authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	Operations Planning and Same Day Operations	Lower	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15</p>	<p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15</p>	<p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15</p>	<p>BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1)</p> <p>OR</p> <p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is</p>	<p>calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)</p>	<p>calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)</p>	<p>privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)</p> <p>OR</p> <p>The Responsible Entity has implemented</p>	<p>complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar</p>	<p>complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar</p>	<p>Information storage locations. (R5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>one or more process(es) to revoke the individual’s user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to</p>	<p>day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)</p>	<p>day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)</p>	<p>requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

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

Examples of possible mechanisms and evidence, when dated, which can be used are:

- 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.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include

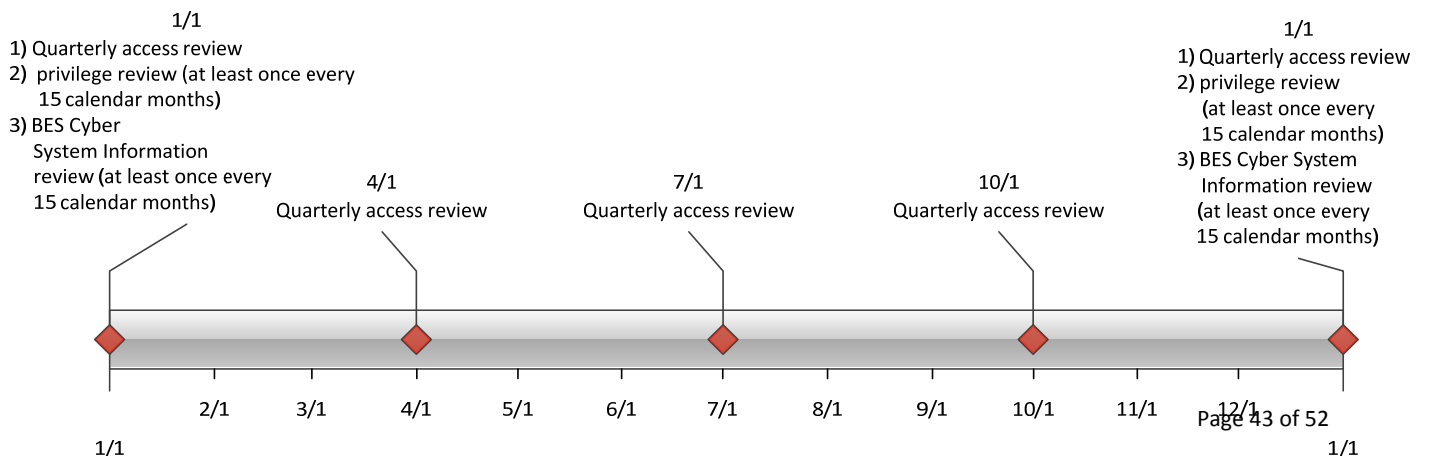
individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

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

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual’s associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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

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

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

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

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

Requirement 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical access "received" ongoing reinforcement – to state that security awareness has been reinforced.

Moved example mechanisms to guidance.

Rationale for R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

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

Summary of Changes:

1. Addition of specific role training for:

- The visitor control program
- Electronic interconnectivity supporting the operation and control of BES Cyber Systems
- Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace “annually” with “once every 15 calendar months.”

Rationale for R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

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

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

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

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

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

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

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a “need to know” basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term “review” entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

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

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

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

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: “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).

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.”

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

*The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards to **require immediate revocation** for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Modified two VSLs in R4.	Errata
5.1	11/22/13	FERC Order issued approving CIP-004-5.1. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-004-5.1 — Cyber Security — Personnel

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-004-5.1	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-5
3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**
 - 4.1.6 **Reliability Coordinator**
 - 4.1.7 **Transmission Operator**

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

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

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

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

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> • PCA Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> • PCA 	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> • PCA 	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.3	<p>Electronic Access Points for High Impact BES Cyber Systems</p> <p>Electronic Access Points for Medium Impact BES Cyber Systems</p>	<p>Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.</p>	<p>An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.</p>
1.4	<p>High Impact BES Cyber Systems with Dial-up Connectivity and their associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:</p> <ul style="list-style-type: none"> • PCA 	<p>Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.</p>	<p>An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.</p>

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

- R2.** Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
- M2.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> • PCA 	<p>Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.</p>	<p>Examples of evidence may include, but are not limited to, network diagrams or architecture documents.</p>
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> • PCA 	<p>For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.</p>	<p>An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.</p>

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> • PCA 	<p>Require multi-factor authentication for all Interactive Remote Access sessions.</p>	<p>An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used.</p> <p>Examples of authenticators may include, but are not limited to,</p> <ul style="list-style-type: none"> • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning and Same Day Operations	Medium			<p>The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)</p>	<p>The Responsible Entity did not document one or more processes for <i>CIP-005-5 Table R1 – Electronic Security Perimeter</i>. (R1)</p> <p>OR</p> <p>The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1)</p> <p>OR</p> <p>External Routable Connectivity through the ESP was not through an identified EAP. (1.2)</p> <p>OR</p> <p>The Responsible Entity did not require inbound and</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2	Operations Planning and Same Day Operations	Medium	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of ‘Associated Protected Cyber Assets’ that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the ‘high water mark’).

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the “high water mark”) where the term “Protected Cyber Assets” is used. The CIP Cyber Security Standards accomplish the “high water mark” by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as “Protected Cyber Assets” of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the

Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

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

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

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

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical “perimeter.”

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point (“EAP”).

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)

Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)

Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)

Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)

Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)

Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in **Guidance for Secure Interactive Remote Access** published by NERC in July 2011.

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

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

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

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)

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

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-005-5 — Cyber Security - Electronic Security Perimeter(s)

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-005-5	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems
2. **Number:** CIP-006-5
3. **Purpose:** To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**
 - 4.1.6 **Reliability Coordinator**

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

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

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

Most requirements open with, *“Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying “implement” as follows:

Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .**

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

documented processes themselves are not required to include the “. . . identifies, assesses, and corrects deficiencies, . . .” elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].
- M1.** Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.1	<p>Medium Impact BES Cyber Systems without External Routable Connectivity</p> <p>Physical Access Control Systems (PACS) associated with:</p> <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.2	<p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.</p>

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.</p>	<p>An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.</p>

CIP-006-5 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.</p>
1.6	<p>Physical Access Control Systems (PACS) associated with:</p> <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	<p>Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.</p>	<p>An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.</p>

CIP-006-5 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.7	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.8	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.</p>	<p>An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.</p>

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.9	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.</p>	<p>An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.</p>

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

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

CIP-006-5 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.</p>	<p>An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.</p>

CIP-006-5 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.</p>	<p>An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Retain visitor logs for at least ninety calendar days.</p>	<p>An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.</p>

- R3.** Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*.
- M3.** Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	Applicable Systems	Requirement	Measures
3.1	<p>Physical Access Control Systems (PACS) associated with:</p> <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity <p>Locally mounted hardware or devices at the Physical Security Perimeter associated with:</p> <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	<p>Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.</p>	<p>An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.</p>

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning Same-Day Operations	Medium	<p>The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8)</p> <p>OR</p> <p>The Responsible Entity has a</p>	<p>The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7)</p> <p>OR</p> <p>The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7)</p> <p>OR</p> <p>The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and</p>	<p>The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5)</p> <p>OR</p> <p>The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5)</p> <p>OR</p> <p>The Responsible Entity</p>	<p>The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1)</p> <p>OR</p> <p>The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify,</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified	identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the	assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)		deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)</p> <p>OR</p> <p>The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)</p> <p>OR</p> <p>The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5)</p> <p>OR</p> <p>The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6)</p> <p>OR</p> <p>The Responsible Entity does not have a process to alert for unauthorized physical access to Physical</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>Access Control Systems or to communicate such alerts within 15 minutes to identified personnel (1.7)</p> <p>OR</p> <p>The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8)</p> <p>OR</p> <p>The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)</p>
R2	Same-Day Operations	Medium	N/A	The Responsible Entity included a visitor control program that requires logging of each	The Responsible Entity included a visitor control program that requires continuous	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>of the initial entry and last exit dates and times of the visitor, the visitor’s name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor’s name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity included a visitor control program to retain visitor logs for at</p>	<p>escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)</p>	<p>requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1)</p> <p>OR</p> <p>The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor’s name, and the point of contact. (2.2)</p> <p>OR</p> <p>The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		
R3	Long Term Planning	Lower	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	did complete required testing within 26 calendar months. (3.1)	did complete required testing within 27 calendar months. (3.1)	has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

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

Requirement R1:

Methods of physical access control include:

- **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 into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting 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.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

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

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

Requirement R3:

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

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4

Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.

FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).

Reference to prior version: (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

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

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

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

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Guidelines and Technical Basis

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-006-5. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-006-5 — Cyber Security - Physical Security of BES Cyber Systems

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-006-5	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-5
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**
 - 4.1.6 **Reliability Coordinator**

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

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

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees’ approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying “implement” as follows:

Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .**

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

documented processes themselves are not required to include the “. . . identifies, assesses, and corrects deficiencies, . . .” elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*. [*Violation Risk Factor: Medium*] [*Time Horizon: Same Day Operations.*]
- M1.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
1.2	<p>High Impact BES Cyber Systems</p> <p>Medium Impact BES Cyber Systems at Control Centers</p>	<p>Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.</p>	<p>An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.</p>

- R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.</p>	<p>An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.</p>

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.</p>	<p>An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.</p>

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:</p> <ul style="list-style-type: none"> • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. <p>Mitigation plans shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.</p>	<p>An example of evidence may include, but is not limited to, records of implementation of mitigations.</p>

- R3.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].
- M3.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Mitigate the threat of detected malicious code.	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

- R4.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]
- M4.** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:</p> <ol style="list-style-type: none"> 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code. 	<p>Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.</p>

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):</p> <ol style="list-style-type: none"> 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging. 	<p>Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.</p>

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.</p>	<p>Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.</p>
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	<p>Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.</p>	<p>Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.</p>

- R5.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M5.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Have a method(s) to enforce authentication of interactive user access, where technically feasible.</p>	<p>An example of evidence may include, but is not limited to, documentation describing how access is authenticated.</p>

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).</p>	<p>An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.</p>

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Identify individuals who have authorized access to shared accounts.</p>	<p>An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.</p>

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Change known default passwords, per Cyber Asset capability	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:</p> <ol style="list-style-type: none"> 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset. 	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.6	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.7	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Where technically feasible, either:</p> <ul style="list-style-type: none"> • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts. 	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Same Day Operations	Medium	N/A	<p>The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2)</p> <p>OR</p> <p>The Responsible Entity has implemented and</p>	<p>The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has implemented and documented processes for determining</p>	<p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 and has identified deficiencies but did not assess or correct the deficiencies. (R1)</p> <p>OR</p> <p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	the deficiencies. (R1)
R2	Operations Planning	Medium	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 and has identified deficiencies but did not assess or correct

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within	sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not	applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR	the deficiencies. (R2) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an</p>	<p>identify, assess, or correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct</p>	<p>The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or</p>	<p>or installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3)</p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a</p>	<p>the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)</p>	<p>more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by</p>	<p>OR</p> <p>The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4)</p> <p>OR</p> <p>The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct	applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by	revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess,	applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				or correct the deficiencies. (2.3)		
R3	Same Day Operations	Medium		<p>The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es), but,</p>	<p>The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected</p>	<p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and has identified deficiencies but did not assess or correct the deficiencies. (R3)</p> <p>OR</p> <p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify,</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR	assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	Same Day Operations and Operations Assessment	Medium	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and has identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined</p>	<p>determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined</p>	<p>responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable</p>	<p>deficiencies but did not assess or correct the deficiencies. (R4)</p> <p>OR</p> <p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)</p>	<p>summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)</p>	<p>Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event</p>	<p>(per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					logs for at least the last 90 consecutive days and has identified deficiencies but did not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not	4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	Operations Planning	Medium	The Responsible Entity has implemented one or more documented process(es) for password-only	The Responsible Entity has implemented one or more documented process(es) for password-only	The Responsible Entity has implemented one or more documented process(es) for System Access	The Responsible Entity did not implement or document one or more process(es) that included the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only</p>	<p>authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only</p>	<p>Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct the deficiencies. (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or</p>	<p>applicable items in <i>CIP-007-5 Table R5</i> and has identified deficiencies but did not assess or correct the deficiencies. (R5)</p> <p>OR</p> <p>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in <i>CIP-007-5 Table R5</i> and did not identify, assess, or correct the deficiencies. (R5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or	enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for</p>	<p>The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to	or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to	parameters described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and has identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible (“listening”) ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset’s function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed ‘needed.’

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only,

which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as

it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include:

(i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports.

The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, \$, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the ‘needed for normal or emergency operations’ to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.

Reference to prior version: (Part 1.1) CIP-007-4, R2.1 and R2.2

Change Rationale: (Part 1.1)

The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of ‘normal or emergency’ added no value and has been removed.

Reference to prior version: (Part 1.2) New

Change Rationale: (Part 1.2)

On March 18, 2010, FERC issued an order to approve NERC’s interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term “ports” in “ports and services” refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Rationale for R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the “release” date was. The current wording stated “document the assessment of security patches and security

upgrades for applicability within thirty calendar days of availability of the patches or upgrades” and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

Reference to prior version: (Part 2.1) CIP-007, R3

Change Rationale: (Part 2.1)

The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.

Reference to prior version: (Part 2.2) CIP-007, R3.1

Change Rationale: (Part 2.2)

Similar to the current wording but added “from the source or sources identified in 2.1” to clarify the 35-day time frame.

Reference to prior version: (Part 2.3) CIP-007, R3.2

Change Rationale: (Part 2.3)

The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.

Reference to prior version: (Part 2.4) CIP-007, R3.2

Change Rationale: (Part 2.4)

Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.

Rationale for R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of

that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method...However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance..."

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Reference to prior version: (Part 3.1) CIP-007-4, R4; CIP-007-4, R4.1

Change Rationale: (Part 3.1)

See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.

Reference to prior version: (Part 3.2) CIP-007-4, R4; CIP-007-4, R4.1

Change Rationale: (Part 3.2)

See the Summary of Changes.

Reference to prior version: (Part 3.3) CIP-007-4, R4; CIP-007-4, R4.2

Change Rationale: (Part 3.3)

Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.

Rationale for R4:

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor.”

The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

Reference to prior version: (Part 4.1) CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3

Change Rationale: (Part 4.1)

This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.

Reference to prior version: (Part 4.2) CIP-005-4, R3.2; CIP-007-4, R6.2

Change Rationale: (Part 4.2)

This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.

Reference to prior version: (Part 4.3) CIP-005-4, R3.2; CIP-007-4, R6.4

Change Rationale: (Part 4.3)

No substantive change.

Reference to prior version: (Part 4.4) CIP-005-4, R3.2; CIP-007-4, R6.5

Change Rationale: (Part 4.4)

Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information.

Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.

Rationale for R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for

true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication

mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

Reference to prior version: (Part 5.1) CIP-007-4, R5

Change Rationale: (Part 5.1)

The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase “that minimize the risk of unauthorized access” was removed and more appropriately captured in the rationale statement.

Reference to prior version: (Part 5.2) CIP-007-4, R5.2 and R5.2.1

Change Rationale: (Part 5.2)

CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.

Reference to prior version: (Part 5.3) CIP-007-4, R5.2.2

Change Rationale: (Part 5.3)

No significant changes. Added “authorized” access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

Reference to prior version: (Part 5.4) CIP-007-4, R5.2.1

Change Rationale: (Part 5.4)

The requirement for the “removal, disabling or renaming of such accounts where possible” has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.

Reference to prior version: (Part 5.5) CIP-007-4, R5.3

Change Rationale: (Part 5.5)

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password

credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.

Reference to prior version: (Part 5.6) CIP-007-4, R5.3.3

Change Rationale: (Part 5.6)

**This was originally Requirement R5.5.3, but moved to add “external routable connectivity” to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

Reference to prior version: (Part 5.7) New Requirement

Change Rationale: (Part 5.7)

Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	

Guidelines and Technical Basis

3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-007-5 — Cyber Security - System Security Management

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-007-5	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-5
3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**
 - 4.1.6 **Reliability Coordinator**
 - 4.1.7 **Transmission Operator**

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-5:

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

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

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

- R1.** Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].
- M1.** Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

- R2.** Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].
- M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: <ul style="list-style-type: none"> • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident. 	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

- R3.** Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident*.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	<p>No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:</p> <p>3.1.1. Document any lessons learned or document the absence of any lessons learned;</p> <p>3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and</p> <p>3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.</p>	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	<p>No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:</p> <p>3.2.1. Update the Cyber Security Incident response plan(s); and</p> <p>3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.</p>	<p>An example of evidence may include, but is not limited to:</p> <ol style="list-style-type: none"> 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning	Lower	N/A	N/A	<p>The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3)</p> <p>OR</p> <p>The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)</p>	<p>The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1)</p> <p>OR</p> <p>The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2)</p> <p>OR</p> <p>The Responsible Entity has developed a Cyber Security Incident response plan, but did</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	Operations Planning Real-time Operations	Lower	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with	The Responsible Entity has not updated the	The Responsible Entity has neither	The Responsible Entity has neither

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)</p>	<p>Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2)</p> <p>OR</p> <p>The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)</p> <p>OR</p>	<p>documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)</p> <p>OR</p> <p>The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2)</p> <p>OR</p> <p>The Responsible Entity has not updated the</p>	<p>documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2)</p> <ul style="list-style-type: none"> • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. 	<p>Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2)</p> <ul style="list-style-type: none"> • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. 	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

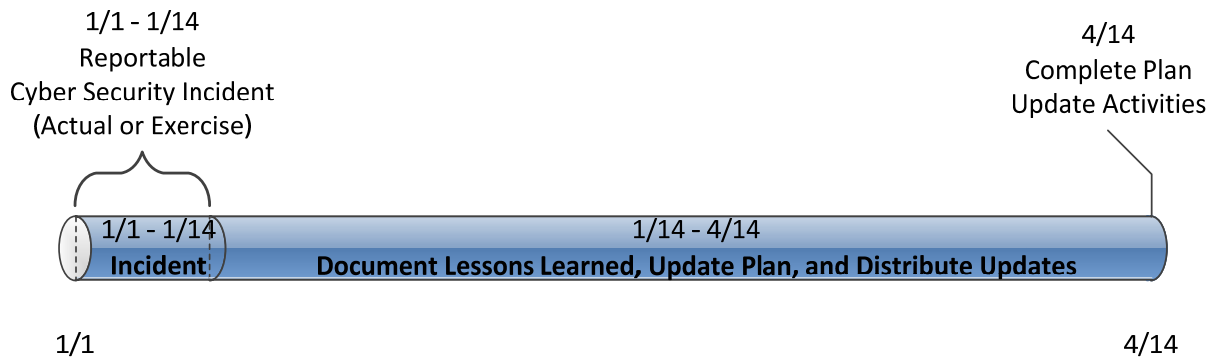


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

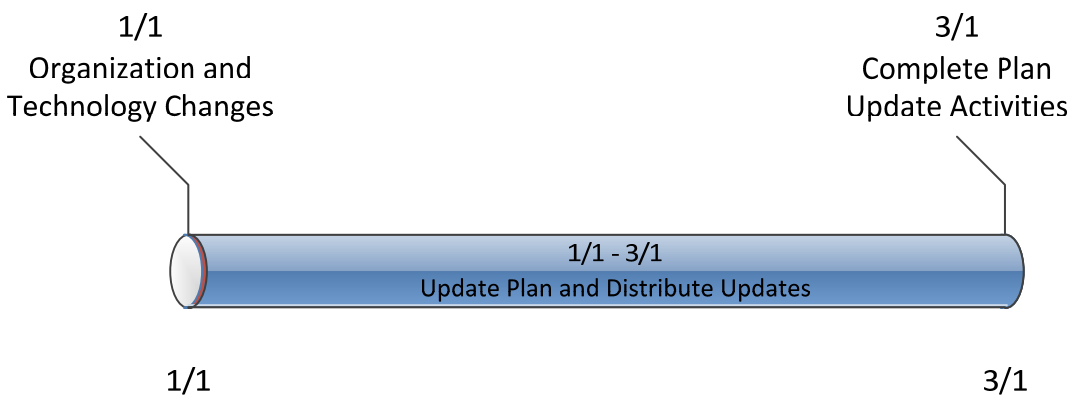


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

“Characterize” has been changed to “identify” for clarity. “Response actions” has been changed to “respond to” for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response “groups or individuals” to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)

Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)

Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the

plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	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.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	

Guidelines and Technical Basis

4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-008-5 — Cyber Security - Incident Reporting and Response Planning

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-008-5	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems
2. **Number:** CIP-009-5
3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**
 - 4.1.6 **Reliability Coordinator**

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-5:

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying “implement” as follows:

Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .**

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

documented processes themselves are not required to include the “. . . identifies, assesses, and corrects deficiencies, . . .” elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

- R1.** Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
- M1.** Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> 1. EACMS; and 2. PACS 	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> 1. EACMS; and 2. PACS 	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>One or more processes for the backup and storage of information required to recover BES Cyber System functionality.</p>	<p>An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.</p>

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.</p>	<p>An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.</p>
1.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.</p>	<p>An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.</p>

- R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]
- M2.** Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing*.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months:</p> <ul style="list-style-type: none"> • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise. 	<p>An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.</p>

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.</p> <p>An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.</p>	<p>An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).</p>
2.3	High Impact BES Cyber Systems	<p>Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.</p> <p>An actual recovery response may substitute for an operational exercise.</p>	<p>Examples of evidence may include, but are not limited to, dated documentation of:</p> <ul style="list-style-type: none"> • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

- R3.** Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].
- M3.** Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>No later than 90 calendar days after completion of a recovery plan test or actual recovery:</p> <ol style="list-style-type: none"> 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned. 	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:</p> <ol style="list-style-type: none"> 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates. 	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	Operations	Lower	The Responsible	The Responsible	The Responsible	The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>Planning</p> <p>Real-time Operations</p>		<p>Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any</p>	<p>Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were</p>	<p>Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1)</p> <p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were</p>	<p>Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1)</p> <p>OR</p> <p>The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>deficiencies were identified, assessed, and corrected. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)</p>	<p>identified, assessed, and corrected. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)</p>	<p>identified, assessed, and corrected. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)</p>	<p>Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2)</p> <p>OR</p> <p>The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity has tested a</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)</p> <p>OR</p> <p>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)</p> <p>OR</p> <p>The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) <ul style="list-style-type: none"> • Roles or responsibilities, or • Responders, or • Technology changes. 	documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) <ul style="list-style-type: none"> • Roles or responsibilities, or • Responders, or • Technology changes. 	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at <http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf>
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

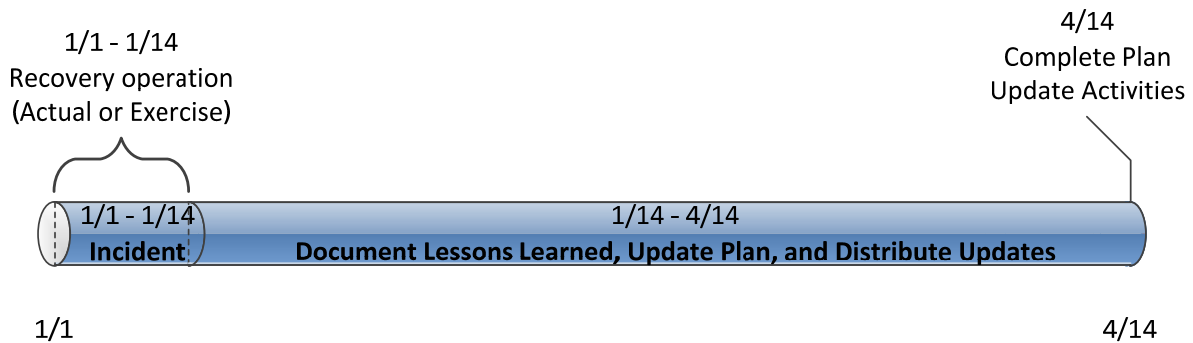


Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

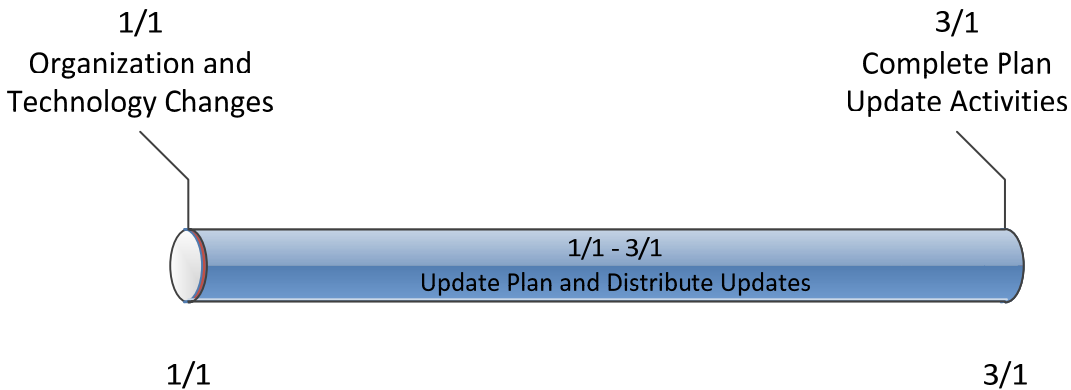


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center”	3/24/06
2	9/30/09	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.	

Guidelines and Technical Basis

3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-009-5 — Cyber Security - Recovery Plans for BES Cyber Systems

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-009-5	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments
2. **Number:** CIP-010-1
3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-1:

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying “implement” as follows:

Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies**, . . .

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

documented processes themselves are not required to include the “. . . identifies, assesses, and corrects deficiencies, . . .” elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately

based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)**– Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)**– Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Develop a baseline configuration, individually or by group, which shall include the following items:</p> <ol style="list-style-type: none"> 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied. 	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Authorize and document changes that deviate from the existing baseline configuration.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.</p>	<p>An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.</p>
1.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>For a change that deviates from the existing baseline configuration:</p> <ol style="list-style-type: none"> 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification. 	<p>An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.</p>

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber Systems	<p>Where technically feasible, for each change that deviates from the existing baseline configuration:</p> <p>1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and</p> <p>1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.</p>	<p>An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.</p>

- R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

- R3.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments*. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]
- M3.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>At least once every 15 calendar months, conduct a paper or active vulnerability assessment.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment;; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems	<p>Where technically feasible, at least once every 36 calendar months:</p> <p>3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and</p> <p>3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.</p>	<p>An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.</p>

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PCA 	<p>Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.</p>	<p>An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.</p>
3.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.</p>	<p>An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).</p>

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	<p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline</p>	<p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and</p>	<p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified</p>	<p>The Responsible Entity has not documented or implemented any configuration change management process(es). (R1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible</p>	<p>identified deficiencies but did not assess and correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has a process(es) to determine required</p>	<p>deficiencies but did not assess and correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has a process(es) that requires authorization and documentation for</p>	<p>implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)</p> <p>OR</p> <p>The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct</p>	<p>security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1)</p> <p>OR</p> <p>The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline</p>	<p>changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)</p> <p>OR</p> <p>The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2)</p> <p>OR</p> <p>The Responsible Entity has a process(es) to update</p>	<p>the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)</p> <p>OR</p> <p>The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)</p> <p>OR</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies in the verification documentation. (1.4.3)	configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the	The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in	required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					<p>CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)</p> <p>OR</p> <p>The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies.</p>	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					(1.5.1) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identified deficiencies but did not assess or correct the deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	Operations Planning	Medium	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						<p>document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1)</p> <p>OR</p> <p>The Responsible Entity has documented and</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	Long-term Planning and Operations Planning	Medium	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>months, since the last assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems.</p>	<p>assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(3.2)			its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset’s baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset’s baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-5. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-5 R2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Reference to prior version: (Part 1.1) New Requirement

Change Rationale: (Part 1.1)

The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.

Reference to prior version: (Part 1.2) CIP-007-3, R9; CIP-003-3, R6

Change Rationale: (Part 1.2)

The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.

Reference to prior version: (Part 1.3) CIP-007-3, R9; CIP-005-3, R5

Change Rationale: (Part 1.3)

Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.

Reference to prior version: (Part 1.4) CIP-007-3, R1

Change Rationale: (Part 1.4)

The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.

Reference to prior version: (Part 1.5) CIP-007-3, R1

Change Rationale: (Part 1.5)

This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.

This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.

Rationale for R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Reference to prior version: (Part 2.1) New Requirement

Change Rationale: (Part 2.1)

The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.

This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.

Thirty-five Calendar days allows for a “once-a-month” frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.

Rationale for R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Reference to prior version: (Part 3.1) CIP-005-4, R4; CIP-007-4, R8

Change Rationale: (Part 3.1)

As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.

Reference to prior version: (Part 3.2) New Requirement

Change Rationale: (Part 3.2)

FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.

As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.

Reference to prior version: (Part 3.3) New Requirement

Change Rationale: (Part 3.3)

FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.

Reference to prior version: (Part 3.4) CIP-005-3, R4.5; CIP-007-3, R8.4

Change Rationale: (Part 3.4)

Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-010-1 — Cyber Security - Configuration Change Management and Vulnerability Assessments

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-010-1	All	04/01/2016	

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-1
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator or Interchange Authority**
 - 4.1.6 **Reliability Coordinator**

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-1:

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

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

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

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees’ approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying “implement” as follows:

Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented

processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the “. . . identifies, assesses, and corrects deficiencies, . . .” elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)**– Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection*. [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning*].
- M1.** Evidence for the information protection program must include the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Method(s) to identify information that meets the definition of BES Cyber System Information.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> • Documented method to identify BES Cyber System Information from entity’s information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity’s information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity’s information protection program.

CIP-011-1 Table R1 – Information Protection			
Part	Applicable Systems	Requirement	Measure
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity’s documented procedure(s).

- R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A		<p>The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1)</p> <p>OR</p> <p>The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify, assess, or correct the</p>	<p>The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					assess, or correct the deficiencies. (1.2)	
R2	Operations Planning	Lower	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity’s information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity’s BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].

Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

Reference to prior version: (Part 1.1) CIP-003-3, R4; CIP-003-3, R4.2

Change Rationale: (Part 1.1)

The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (e.g., confidential, public, internal use only, etc.) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.

Reference to prior version: (Part 1.2) CIP-003-3, R4

Change Rationale: (Part 1.2)

The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.

Rationale for R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

Reference to prior version: (Part 2.1) CIP-007-3, R7.2

Change Rationale: (Part 2.1)

Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal.

Reference to prior version: (Part 2.2) CIP-007-3, R7.1

Change Rationale: (Part 2.2)

Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal.

The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-011-1 — Cyber Security - Information Protection

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-011-1	All	04/01/2016	

A. Introduction

- 1. Title:** Automatic Generation Control
- 2. Number:** BAL-005-0.2b
- 3. Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.
- 4. Applicability:**
 - 4.1.** Balancing Authorities
 - 4.2.** Generator Operators
 - 4.3.** Transmission Operators
 - 4.4.** Load Serving Entities
- 5. Effective Date:** May 13, 2009

B. Requirements

- R1.** All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.
 - R1.1.** Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.
 - R1.2.** Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.
 - R1.3.** Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.
- R2.** Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retirement approved by FERC effective January 21, 2014.)
- R3.** A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.
- R4.** A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.
- R5.** A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.
- R6.** The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

- R7.** The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.
- R8.** The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.
- R8.1.** Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.
- R9.** The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.
- R9.1.** Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.
- R10.** The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.
- R11.** Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.
- R12.** Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.
- R12.1.** Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.
- R12.2.** Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.
- R12.3.** Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.
- R13.** Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.
- R14.** The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.
- R15.** The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

R16. The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

1.1.1. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.

1.1.2. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

1.3.1. Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.

1.3.2. Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

Standard BAL-005-0.2b — Automatic Generation Control

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

- Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added “1.”; changed hyphen to “en dash.” Changed font style for “Appendix 1” to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to “0.1b”	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from “BAL-005-1” to “BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
0.2b	November 21, 2013	R2 and associated elements approved by FERC	

		for retirement as part of the Paragraph 81 project (Project 2013-02) effective January 21, 2014.	
--	--	--	--

Appendix 1

Effective Date: August 27, 2008 (U.S.)

Interpretation of BAL-005-0 Automatic Generation Control, R17

Request for Clarification received from PGE on July 31, 2007

PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

BAL-005-0

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25% of full scale
Remote terminal unit	≤ 0.25% of full scale
Potential transformer	≤ 0.30% of full scale
Current transformer	≤ 0.50% of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to “annually check and calibrate” does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to “annually check and calibrate” the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system operator. Frequency inputs from other sources that are for reference only are excluded. The time error and

Standard BAL-005-0.2b — Automatic Generation Control

frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

* FOR INFORMATIONAL PURPOSES ONLY *

Enforcement Dates: Standard BAL-005-0.2b — Automatic Generation Control

United States

Standard	Requirement	Enforcement Date	Inactive Date
BAL-005-0.2b	R1.	09/13/2012	
BAL-005-0.2b	R1.1.	09/13/2012	
BAL-005-0.2b	R1.2.	09/13/2012	
BAL-005-0.2b	R1.3.	09/13/2012	
BAL-005-0.2b	R2.	09/13/2012	01/21/2014
BAL-005-0.2b	R3.	09/13/2012	
BAL-005-0.2b	R4.	09/13/2012	
BAL-005-0.2b	R5.	09/13/2012	
BAL-005-0.2b	R6.	09/13/2012	
BAL-005-0.2b	R7.	09/13/2012	
BAL-005-0.2b	R8.	09/13/2012	
BAL-005-0.2b	R8.1.	09/13/2012	
BAL-005-0.2b	R9.	09/13/2012	
BAL-005-0.2b	R9.1.	09/13/2012	
BAL-005-0.2b	R10.	09/13/2012	
BAL-005-0.2b	R11.	09/13/2012	
BAL-005-0.2b	R12.	09/13/2012	
BAL-005-0.2b	R12.1.	09/13/2012	
BAL-005-0.2b	R12.2.	09/13/2012	
BAL-005-0.2b	R12.3.	09/13/2012	
BAL-005-0.2b	R13.	09/13/2012	
BAL-005-0.2b	R14.	09/13/2012	
BAL-005-0.2b	R15.	09/13/2012	
BAL-005-0.2b	R16.	09/13/2012	
BAL-005-0.2b	R17.	09/13/2012	

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-3
3. **Purpose:** Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-003-3, “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-003-3:
 - 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-002-3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-3 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-002-3 through CIP-009-3, 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. (Retirement approved by FERC effective January 21, 2014.)
- 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-002-3 through CIP-009-3.

 - 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-002-3 through CIP-009-3, 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). (Retirement approved by FERC effective January 21, 2014.)

 - 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). (Retirement approved by FERC effective January 21, 2014.)
 - R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retirement approved by FERC effective January 21, 2014.)
 - 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. (Retirement approved by FERC effective January 21, 2014.)
- 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-002-3, 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. (Retirement approved by FERC effective January 21, 2014.)
 - 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. (Retirement approved by FERC effective January 21, 2014.)
- 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. (Retirement approved by FERC effective January 21, 2014.)
- 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).	

Standard CIP-003-3 — Cyber Security — Security Management Controls

		Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Adopted by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
3	2/7/13	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
3	11/21/13	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-003-3 — Cyber Security - Security Management Controls

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-003-3	R1.	10/01/2010	03/31/2016
CIP-003-3	R1.1.	10/01/2010	03/31/2016
CIP-003-3	R1.2.	10/01/2010	01/21/2014
CIP-003-3	R1.3.	10/01/2010	03/31/2016
CIP-003-3	R2.	10/01/2010	03/31/2016
CIP-003-3	R2.1.	10/01/2010	03/31/2016
CIP-003-3	R2.2.	10/01/2010	03/31/2016
CIP-003-3	R2.3.	10/01/2010	03/31/2016
CIP-003-3	R2.4.	10/01/2010	03/31/2016
CIP-003-3	R3.	10/01/2010	01/21/2014
CIP-003-3	R3.1.	10/01/2010	01/21/2014
CIP-003-3	R3.2.	10/01/2010	01/21/2014
CIP-003-3	R3.3.	10/01/2010	01/21/2014
CIP-003-3	R4.	10/01/2010	03/31/2016
CIP-003-3	R4.1.	10/01/2010	03/31/2016
CIP-003-3	R4.2.	10/01/2010	01/21/2014
CIP-003-3	R4.3.	10/01/2010	03/31/2016
CIP-003-3	R5.	10/01/2010	03/31/2016
CIP-003-3	R5.1.	10/01/2010	03/31/2016
CIP-003-3	R5.1.1.	10/01/2010	03/31/2016
CIP-003-3	R5.1.2.	10/01/2010	03/31/2016
CIP-003-3	R5.2.	10/01/2010	03/31/2016
CIP-003-3	R5.3.	10/01/2010	03/31/2016
CIP-003-3	R6.	10/01/2010	03/31/2016

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-4
3. **Purpose:** Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-003-4, “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-003-4:
 - 4.2.1 Facilities regulated by 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 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54
 - 4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.
5. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth 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-002-4 through CIP-009-4, 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. (Retirement approved by FERC effective January 21, 2014.)
- 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-002-4 through CIP-009-4.
 - 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-002-4 through CIP-009-4, 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). (Retirement approved by FERC effective January 21, 2014.)
 - 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). (Retirement approved by FERC effective January 21, 2014.)
 - R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retirement approved by FERC effective January 21, 2014.)
 - 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. (Retirement approved by FERC effective January 21, 2014.)
- 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-002-4, 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. (Retirement approved by FERC effective January 21, 2014.)

- 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. (Retirement approved by FERC effective January 21, 2014.)
- 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. (Retirement approved by FERC effective January 21, 2014.)
- 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

1.2. The RE shall serve as the CEA with the following exceptions:

- 1.2.1** For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- 1.2.2** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 1.2.3** For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- 1.2.4** For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

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

Standard CIP-003-4 — Cyber Security — Security Management Controls

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2. (Retirement approved by FERC effective January 21, 2014.)	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND

Standard CIP-003-4 — Cyber Security — Security Management Controls

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	changes to the delegated authority are not documented within thirty calendar days of the effective date.
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3. <i>(Retirement approved by FERC effective January 21, 2014.)</i>	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1. <i>(Retirement approved by FERC effective January 21, 2014.)</i>	LOWER	Exceptions to the Responsible Entity’s cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity’s cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity’s cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity’s cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
R3.2. <i>(Retirement approved by FERC effective January 21, 2014.)</i>	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3. <i>(Retirement approved by FERC effective January 21, 2014.)</i>	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.

Standard CIP-003-4 — Cyber Security — Security Management Controls

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
R4.2. (Retirement approved by FERC effective January 21, 2014.)	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not 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.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	<p>The Responsible Entity has established but not documented a change control process</p> <p>OR</p> <p>The Responsible Entity has established but not documented a configuration management process.</p>	<p>The Responsible Entity has established but not documented both a change control process and configuration management process.</p>	<p>The Responsible Entity has not established and documented a change control process</p> <p>OR</p> <p>The Responsible Entity has not established and documented a configuration management process.</p>	<p>The Responsible Entity has not established and documented a change control process</p> <p>AND</p> <p>The Responsible Entity has not established and documented a configuration management process.</p>

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets.</p> <p>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).</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	<p>FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012)</p> <p>Added approved VRF/VSL table to section D.2.</p>	
3, 4	2/7/13	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
4	8/12/13	FERC Order issued granting an extension of time on CIP V4 Reliability Standards. This order extends the enforcement date from April 1, 2014 to October 1, 2014.	
4	11/21/13	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project	

	(Project 2013-02)	
--	-------------------	--

* FOR INFORMATIONAL PURPOSES ONLY *

Enforcement Dates: Standard CIP-003-4 — Cyber Security - Security Management Controls

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-003-4	R1.	10/01/2014	02/03/2014
CIP-003-4	R1.1.	10/01/2014	02/03/2014
CIP-003-4	R1.2.	10/01/2014	01/21/2014
CIP-003-4	R1.3.	10/01/2014	02/03/2014
CIP-003-4	R2.	10/01/2014	02/03/2014
CIP-003-4	R2.1.	10/01/2014	02/03/2014
CIP-003-4	R2.2.	10/01/2014	02/03/2014
CIP-003-4	R2.3.	10/01/2014	02/03/2014
CIP-003-4	R2.4.	10/01/2014	02/03/2014
CIP-003-4	R3.	10/01/2014	01/21/2014
CIP-003-4	R3.1.	10/01/2014	01/21/2014
CIP-003-4	R3.2.	10/01/2014	01/21/2014
CIP-003-4	R3.3.	10/01/2014	01/21/2014
CIP-003-4	R4.	10/01/2014	02/03/2014
CIP-003-4	R4.1.	10/01/2014	02/03/2014
CIP-003-4	R4.2.	10/01/2014	01/21/2014
CIP-003-4	R4.3.	10/01/2014	02/03/2014
CIP-003-4	R5.	10/01/2014	02/03/2014
CIP-003-4	R5.1.	10/01/2014	02/03/2014
CIP-003-4	R5.1.1.	10/01/2014	02/03/2014
CIP-003-4	R5.1.2.	10/01/2014	02/03/2014
CIP-003-4	R5.2.	10/01/2014	02/03/2014
CIP-003-4	R5.3.	10/01/2014	02/03/2014
CIP-003-4	R6.	10/01/2014	02/03/2014

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-3a
3. **Purpose:** Standard CIP-005-3 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-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
4. **Applicability**
 - 4.1. Within the text of Standard CIP-005-3, “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-005-3:
 - 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-002-3, 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-005-3.
- 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 specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.
- 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-004-3 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. (Retirement approved by FERC effective January 21, 2014.)
- 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-005-3.
 - R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 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-008-3.

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-008-3, 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-005-3 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		<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>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).</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation
3a	02/02/11	Approved by FERC	
3a	2/7/13	R2.6 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
3a	11/21/13	R2.6 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
<p>Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.</p> <p>Requirement 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).</p>
Question 1 (Section 4.2.2)
<p>What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?</p>
Response to Question 1
<p>In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.</p>
Question 2 (Section 4.2.2)
<p>Is the communication link physical or logical? Where does it begin and terminate?</p>
Response to Question 2
<p>The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.</p>
Question 3 (Requirement R1.3)
<p>Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?</p>
Response to Question 3
<p>The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.</p>
Question 4 (Requirement R1.3)
<p>If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal</p>

Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?

Response to Question 4

In the case where the "endpoint" is defined as logical and is \geq layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-005-3a — Cyber Security - Electronic Security Perimeter(s)

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-005-3a	R1.	02/02/2011	03/31/2016
CIP-005-3a	R1.1.	02/02/2011	03/31/2016
CIP-005-3a	R1.2.	02/02/2011	03/31/2016
CIP-005-3a	R1.3.	02/02/2011	03/31/2016
CIP-005-3a	R1.4.	02/02/2011	03/31/2016
CIP-005-3a	R1.5.	02/02/2011	03/31/2016
CIP-005-3a	R1.6.	02/02/2011	03/31/2016
CIP-005-3a	R2.	02/02/2011	03/31/2016
CIP-005-3a	R2.1.	02/02/2011	03/31/2016
CIP-005-3a	R2.2.	02/02/2011	03/31/2016
CIP-005-3a	R2.3.	02/02/2011	03/31/2016
CIP-005-3a	R2.4.	02/02/2011	03/31/2016
CIP-005-3a	R2.5.	02/02/2011	03/31/2016
CIP-005-3a	R2.5.1.	02/02/2011	03/31/2016
CIP-005-3a	R2.5.2.	02/02/2011	03/31/2016
CIP-005-3a	R2.5.3.	02/02/2011	03/31/2016
CIP-005-3a	R2.5.4.	02/02/2011	03/31/2016
CIP-005-3a	R2.6.	02/02/2011	01/21/2014
CIP-005-3a	R3.	02/02/2011	03/31/2016
CIP-005-3a	R3.1.	02/02/2011	03/31/2016
CIP-005-3a	R3.2.	02/02/2011	03/31/2016
CIP-005-3a	R4.	02/02/2011	03/31/2016
CIP-005-3a	R4.1.	02/02/2011	03/31/2016
CIP-005-3a	R4.2.	02/02/2011	03/31/2016
CIP-005-3a	R4.3.	02/02/2011	03/31/2016
CIP-005-3a	R4.4.	02/02/2011	03/31/2016
CIP-005-3a	R4.5.	02/02/2011	03/31/2016
CIP-005-3a	R5.	02/02/2011	03/31/2016
CIP-005-3a	R5.1.	02/02/2011	03/31/2016

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-005-3a — Cyber Security - Electronic Security Perimeter(s)

United States

CIP-005-3a	R5.2.	02/02/2011	03/31/2016
CIP-005-3a	R5.3.	02/02/2011	03/31/2016

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-4a
3. **Purpose:** Standard CIP-005-4a 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-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability**
 - 4.1. Within the text of Standard CIP-005-4a, “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-005-4a:
 - 4.2.1 Facilities regulated by 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-002-4, identify that they have no Critical Cyber Assets.
 - 4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.
5. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption 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-005-4a.
- 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 specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
- 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-004-4 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. (Retirement approved by FERC effective January 21, 2014.)

- 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-005-4a.
 - R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a 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-008-4.

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

1.2. The RE shall serve as the CEA with the following exceptions:

- 1.2.1** For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- 1.2.1** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 1.2.1** For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- 1.2.2** For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

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-008-4, 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-005-4a 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

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	and Standard CIP-009-4.	and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not 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).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor 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.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter.		
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6. (Retirement approved by FERC effective January 21, 2014.)	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.			
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to designated response personnel.	Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

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	Approved by NERC Board of Trustees 5/6/09	<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>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).</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	Revised.
3	12/16/09	<p>Changed CIP-005-2 to CIP-005-3.</p> <p>Changed all references to CIP Version “2” standards to CIP Version “3” standards.</p> <p>For Violation Severity Levels, changed, “To be developed later” to “Developed separately.”</p>	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	<p>Update to conform to changes to CIP-002-4 (Project 2008-06)</p> <p>Update version number from “3” to “4a”</p>
4a	4/19/12	<p>FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012)</p> <p>Added approved VRF/VSL table to section D.2.</p>	
3a, 4a	2/7/13	R2.6 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	

Standard CIP-005-4a — Cyber Security — Electronic Security Perimeter(s)

4a	8/12/13	FERC Order issued granting an extension of time on CIP V4 Reliability Standards. This order extends the enforcement date from April 1, 2014 to October 1, 2014.	
4a	11/21/13	R2.6 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
<p>Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.</p> <p>Requirement 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).</p>
Question 1 (Section 4.2.2)
<p>What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?</p>
Response to Question 1
<p>In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.</p>
Question 2 (Section 4.2.2)
<p>Is the communication link physical or logical? Where does it begin and terminate?</p>
Response to Question 2
<p>The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.</p>
Question 3 (Requirement R1.3)
<p>Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?</p>
Response to Question 3
<p>The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.</p>
Question 4 (Requirement R1.3)
<p>If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are</p>

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?

Response to Question 4

In the case where the "endpoint" is defined as logical and is \geq layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."

* FOR INFORMATIONAL PURPOSES ONLY *

Enforcement Dates: Standard CIP-005-4a — Cyber Security - Electronic Security Perimeter(s)

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-005-4a	R1.	10/01/2014	02/03/2014
CIP-005-4a	R1.1.	10/01/2014	02/03/2014
CIP-005-4a	R1.2.	10/01/2014	02/03/2014
CIP-005-4a	R1.3.	10/01/2014	02/03/2014
CIP-005-4a	R1.4.	10/01/2014	02/03/2014
CIP-005-4a	R1.5.	10/01/2014	02/03/2014
CIP-005-4a	R1.6.	10/01/2014	02/03/2014
CIP-005-4a	R2.	10/01/2014	02/03/2014
CIP-005-4a	R2.1.	10/01/2014	02/03/2014
CIP-005-4a	R2.2.	10/01/2014	02/03/2014
CIP-005-4a	R2.3.	10/01/2014	02/03/2014
CIP-005-4a	R2.4.	10/01/2014	02/03/2014
CIP-005-4a	R2.5.	10/01/2014	02/03/2014
CIP-005-4a	R2.5.1.	10/01/2014	02/03/2014
CIP-005-4a	R2.5.2.	10/01/2014	02/03/2014
CIP-005-4a	R2.5.3.	10/01/2014	02/03/2014
CIP-005-4a	R2.5.4.	10/01/2014	02/03/2014
CIP-005-4a	R2.6.	10/01/2014	01/21/2014
CIP-005-4a	R3.	10/01/2014	02/03/2014
CIP-005-4a	R3.1.	10/01/2014	02/03/2014
CIP-005-4a	R3.2.	10/01/2014	02/03/2014
CIP-005-4a	R4.	10/01/2014	02/03/2014
CIP-005-4a	R4.1.	10/01/2014	02/03/2014
CIP-005-4a	R4.2.	10/01/2014	02/03/2014
CIP-005-4a	R4.3.	10/01/2014	02/03/2014
CIP-005-4a	R4.4.	10/01/2014	02/03/2014
CIP-005-4a	R4.5.	10/01/2014	02/03/2014
CIP-005-4a	R5.	10/01/2014	02/03/2014
CIP-005-4a	R5.1.	10/01/2014	02/03/2014

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-005-4a — Cyber Security - Electronic Security Perimeter(s)

United States

CIP-005-4a	R5.2.	10/01/2014	02/03/2014
CIP-005-4a	R5.3.	10/01/2014	02/03/2014

A. Introduction

1. **Title:** Cyber Security — Systems Security Management
2. **Number:** CIP-007-3a
3. **Purpose:** Standard CIP-007-3 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-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-007-3, “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-007-3:
 - 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-002-3, 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-007-3, 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-003-3 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-003-3 Requirement R5.

- 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. (Retirement approved by FERC effective January 21, 2014.)
- 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-007-3 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-008-3 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. Rerwording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
2	05/06/09	Adopted by NERC Board of Trustees	Revised
2a	11/05/09	Added Appendix 1 — Interpretation of R2 approved by BOT on November 5, 2009	Interpretation
2a	03/18/10	Interpretation of CIP-007-1 Requirement R2 — FERC Approved, per footnote 11 of Order — to be appended to CIP-007-2, Effective Date April 1, 2010	Interpretation
3		Updated version numbers from -2 to -3	
3	12/16/09	Adopted by the NERC Board of Trustees	
3	2/07/13	R7.3 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
3a	5/13/13	Added FERC approved interpretation of R2 (should have been appended to CIP-007-3 when the interpretation was approved by FERC)	Interpretation
3a	11/21/13	R7.3 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
R2. 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.
Question
Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?
Response
The drafting team interprets the term “ports” used as part of the phrase “ports and services” to refer to logical ports, e.g., Transmission Control Protocol (TCP) ports, where interface with communication services occurs.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-007-3a — Cyber Security — Systems Security Management

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-007-3a	R1.	10/01/2010	03/31/2016
CIP-007-3a	R1.1.	10/01/2010	03/31/2016
CIP-007-3a	R1.2.	10/01/2010	03/31/2016
CIP-007-3a	R1.3.	10/01/2010	03/31/2016
CIP-007-3a	R2.	10/01/2010	03/31/2016
CIP-007-3a	R2.1.	10/01/2010	03/31/2016
CIP-007-3a	R2.2.	10/01/2010	03/31/2016
CIP-007-3a	R2.3.	10/01/2010	03/31/2016
CIP-007-3a	R3.	10/01/2010	03/31/2016
CIP-007-3a	R3.1.	10/01/2010	03/31/2016
CIP-007-3a	R3.2.	10/01/2010	03/31/2016
CIP-007-3a	R4.	10/01/2010	03/31/2016
CIP-007-3a	R4.1.	10/01/2010	03/31/2016
CIP-007-3a	R4.2.	10/01/2010	03/31/2016
CIP-007-3a	R5.	10/01/2010	03/31/2016
CIP-007-3a	R5.1.	10/01/2010	03/31/2016
CIP-007-3a	R5.1.1.	10/01/2010	03/31/2016
CIP-007-3a	R5.1.2.	10/01/2010	03/31/2016
CIP-007-3a	R5.1.3.	10/01/2010	03/31/2016
CIP-007-3a	R5.2.	10/01/2010	03/31/2016
CIP-007-3a	R5.2.1.	10/01/2010	03/31/2016
CIP-007-3a	R5.2.2.	10/01/2010	03/31/2016
CIP-007-3a	R5.2.3.	10/01/2010	03/31/2016
CIP-007-3a	R5.3.	10/01/2010	03/31/2016
CIP-007-3a	R5.3.1.	10/01/2010	03/31/2016
CIP-007-3a	R5.3.2.	10/01/2010	03/31/2016
CIP-007-3a	R5.3.3.	10/01/2010	03/31/2016
CIP-007-3a	R6.	10/01/2010	03/31/2016
CIP-007-3a	R6.1.	10/01/2010	03/31/2016

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-007-3a — Cyber Security — Systems Security Management

United States

CIP-007-3a	R6.2.	10/01/2010	03/31/2016
CIP-007-3a	R6.3.	10/01/2010	03/31/2016
CIP-007-3a	R6.4.	10/01/2010	03/31/2016
CIP-007-3a	R6.5.	10/01/2010	03/31/2016
CIP-007-3a	R7.	10/01/2010	03/31/2016
CIP-007-3a	R7.1.	10/01/2010	03/31/2016
CIP-007-3a	R7.2.	10/01/2010	03/31/2016
CIP-007-3a	R7.3.	10/01/2010	01/21/2014
CIP-007-3a	R8.	10/01/2010	03/31/2016
CIP-007-3a	R8.1.	10/01/2010	03/31/2016
CIP-007-3a	R8.2.	10/01/2010	03/31/2016
CIP-007-3a	R8.3.	10/01/2010	03/31/2016
CIP-007-3a	R8.4.	10/01/2010	03/31/2016
CIP-007-3a	R9.	10/01/2010	03/31/2016

A. Introduction

1. **Title:** Cyber Security — Systems Security Management
2. **Number:** CIP-007-4a
3. **Purpose:** Standard CIP-007-4 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-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-007-4, “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-007-4:
 - 4.2.1 Facilities regulated by 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 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54
 - 4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.
5. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth 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-007-4, 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-003-4 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-003-4 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-003-4 Requirement R5 and Standard CIP-004-4 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-008-4.
 - 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-005-4.
 - 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. (Retirement approved by FERC effective January 21, 2014.)
- 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-007-4 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

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

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-008-4 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

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, but did not document that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).

Standard CIP-007-4a — Cyber Security — Systems Security Management

R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.
R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, 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).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, 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).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, 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.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.

Standard CIP-007-4a — Cyber Security — Systems Security Management

		after the availability of the patches and upgrades.			
R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.

Standard CIP-007-4a — Cyber Security — Systems Security Management

			access authentication of, and accountability for, all user activity.		
R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not 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.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not 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.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual),	Where such accounts must be shared, the Responsible Entity does not 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).

			with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

Standard CIP-007-4a — Cyber Security — Systems Security Management

			on all Cyber Assets within the Electronic Security Perimeter.		
R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 but did not maintain records as specified in R7.3. <i>(Retirement approved by effective January 21, 2014.)</i>	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or 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-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A

Standard CIP-007-4a — Cyber Security — Systems Security Management

R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3. (Retirement approved by FERC effective January 21, 2014.)	LOWER	N/A	N/A	N/A	N/A
R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A
R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment and acceptance of risk.</p> <p>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.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>R9 changed ninety (90) days to thirty (30) days</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
2	05/06/09	Adopted by NERC Board of Trustees	Revised
2a	11/05/09	Added Appendix 1 — Interpretation of R2 approved by BOT on November 5, 2009	Interpretation
2a	03/18/10	Interpretation of CIP-007-1 Requirement R2 — FERC Approved, per footnote 11 of Order — to be appended to CIP-007-2, Effective Date April 1, 2010	Interpretation
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
3	2/7/13	R7.3 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
3a	3/23/12	Added FERC approved interpretation of R2 (should have been appended to CIP-007-3 when the interpretation was approved by FERC)	Interpretation
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	<p>FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012)</p> <p>Added approved VRF/VSL table to section D.2.</p>	

Standard CIP-007-4a — Cyber Security — Systems Security Management

3, 4	2/7/13	R7.3 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
4a	5/13/13	Added FERC approved interpretation of R2 (should have been appended to CIP-007-4 when the interpretation was approved by FERC)	Interpretation
4a	8/12/13	FERC Order issued granting an extension of time on CIP V4 Reliability Standards. This order extends the enforcement date from April 1, 2014 to October 1, 2014.	
4a	11/21/13	R7.3 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
R2. 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.
Question
Does the term "port" mean a physical (hardware) or a logical (software) connection to a computer?
Response
The drafting team interprets the term “ports” used as part of the phrase “ports and services” to refer to logical ports, e.g., Transmission Control Protocol (TCP) ports, where interface with communication services occurs.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-007-4a — Cyber Security — Systems Security Management

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-007-4a	R1.	10/01/2014	02/03/2014
CIP-007-4a	R1.1.	10/01/2014	02/03/2014
CIP-007-4a	R1.2.	10/01/2014	02/03/2014
CIP-007-4a	R1.3.	10/01/2014	02/03/2014
CIP-007-4a	R2.	10/01/2014	02/03/2014
CIP-007-4a	R2.1.	10/01/2014	02/03/2014
CIP-007-4a	R2.2.	10/01/2014	02/03/2014
CIP-007-4a	R2.3.	10/01/2014	02/03/2014
CIP-007-4a	R3.	10/01/2014	02/03/2014
CIP-007-4a	R3.1.	10/01/2014	02/03/2014
CIP-007-4a	R3.2.	10/01/2014	02/03/2014
CIP-007-4a	R4.	10/01/2014	02/03/2014
CIP-007-4a	R4.1.	10/01/2014	02/03/2014
CIP-007-4a	R4.2.	10/01/2014	02/03/2014
CIP-007-4a	R5.	10/01/2014	02/03/2014
CIP-007-4a	R5.1.	10/01/2014	02/03/2014
CIP-007-4a	R5.1.1.	10/01/2014	02/03/2014
CIP-007-4a	R5.1.2.	10/01/2014	02/03/2014
CIP-007-4a	R5.1.3.	10/01/2014	02/03/2014
CIP-007-4a	R5.2.	10/01/2014	02/03/2014
CIP-007-4a	R5.2.1.	10/01/2014	02/03/2014
CIP-007-4a	R5.2.2.	10/01/2014	02/03/2014
CIP-007-4a	R5.2.3.	10/01/2014	02/03/2014
CIP-007-4a	R5.3.	10/01/2014	02/03/2014
CIP-007-4a	R5.3.1.	10/01/2014	02/03/2014
CIP-007-4a	R5.3.2.	10/01/2014	02/03/2014
CIP-007-4a	R5.3.3.	10/01/2014	02/03/2014
CIP-007-4a	R6.	10/01/2014	02/03/2014
CIP-007-4a	R6.1.	10/01/2014	02/03/2014

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-007-4a — Cyber Security — Systems Security Management

United States

CIP-007-4a	R6.2.	10/01/2014	02/03/2014
CIP-007-4a	R6.3.	10/01/2014	02/03/2014
CIP-007-4a	R6.4.	10/01/2014	02/03/2014
CIP-007-4a	R6.5.	10/01/2014	02/03/2014
CIP-007-4a	R7.	10/01/2014	02/03/2014
CIP-007-4a	R7.1.	10/01/2014	02/03/2014
CIP-007-4a	R7.2.	10/01/2014	02/03/2014
CIP-007-4a	R7.3.	10/01/2014	01/21/2014
CIP-007-4a	R8.	10/01/2014	02/03/2014
CIP-007-4a	R8.1.	10/01/2014	02/03/2014
CIP-007-4a	R8.2.	10/01/2014	02/03/2014
CIP-007-4a	R8.3.	10/01/2014	02/03/2014
CIP-007-4a	R8.4.	10/01/2014	02/03/2014
CIP-007-4a	R9.	10/01/2014	02/03/2014

A. Introduction

1. **Title:** System Restoration from Blackstart Resources
2. **Number:** EOP-005-2
3. **Purpose:** Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.
4. **Applicability:**
 - 4.1. Transmission Operators.
 - 4.2. Generator Operators.
 - 4.3. Transmission Owners identified in the Transmission Operators restoration plan.
 - 4.4. Distribution Providers identified in the Transmission Operators restoration plan.
5. **Proposed Effective Date:** Twenty-four months after the first day of the first calendar quarter following applicable regulatory approval. In those jurisdictions where no regulatory approval is required, all requirements go into effect twenty-four months after Board of Trustees adoption.

B. Requirements

- R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Violation Risk Factor = High] [Time Horizon = Operations Planning]*
 - R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.
 - R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.
 - R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.
 - R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.
 - R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.
 - R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

- R1.7.** Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.
- R1.8.** Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.
- R1.9.** Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.
- R2.** Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R3.** Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
 - R3.1.** If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary. (Retirement approved by FERC effective January 21, 2014.)
- R4.** Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
 - R4.1.** Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.
- R5.** Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*
- R6.** Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify: *[Violation Risk Factor = Medium] [Time Horizon = Long-term Planning]*
 - R6.1.** The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.
 - R6.2.** The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

- R6.3.** The capability of generating resources required to control voltages and frequency within acceptable operating limits.
- R7.** Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration. *[Violation Risk Factor = High] [Time Horizon = Real-time Operations]*
- R8.** Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator. *[Violation Risk Factor = High] [Time Horizon = Real-time Operations]*
- R9.** Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R9.1.** The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.
- R9.2.** A list of required tests including:
- R9.2.1.** The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.
- R9.2.2.** The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.
- R9.3.** The minimum duration of each of the required tests.
- R10.** Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R10.1.** System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.
- R10.2.** Restoration priorities.
- R10.3.** Building of cranking paths.
- R10.4.** Synchronizing (re-energized sections of the System).

- R11.** Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator’s restoration plan that are outside of their normal tasks. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R12.** Each Transmission Operator shall participate in its Reliability Coordinator’s restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R13.** Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R14.** Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R15.** Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator’s restoration plan within 24 hours following such change. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R16.** Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R16.1.** Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R9.
- R16.2.** Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.
- R17.** Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*
- R17.1.** System restoration plan including coordination with the Transmission Operator.
- R17.2.** The procedures documented in Requirement R14.

- R18.** Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator. [*Violation Risk Factor = Medium*] [*Time Horizon = Operations Planning*]

C. Measures

- M1.** Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator.
- M2.** Each Transmission Operator shall have evidence such as e-mails with receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan in accordance with Requirement R2.
- M3.** Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, e-mails with receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.
- M4.** Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, e-mails with receipts, or registered mail receipts, that it has updated its restoration plan and submitted it to its Reliability Coordinator in accordance with Requirement R4.
- M5.** Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan available in its primary and backup control rooms and its System Operators prior to its implementation date in accordance with Requirement R5.
- M6.** Each Transmission Operator shall have documentation such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.
- M7.** If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved shall have evidence such as voice recordings, e-mail, dated computer printouts, or operator logs, that it implemented its restoration plan or restoration plan strategies in accordance with Requirement R7.
- M8.** If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved in such an event shall have evidence, such as voice recordings, e-mail, dated computer printouts, or operator logs, that it resynchronized shut down areas in accordance with Requirement R8.
- M9.** Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R9.
- M10.** Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R10.

- M11.** Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R11.
- M12.** Each Transmission Operator shall have evidence, such as training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R12.
- M13.** Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R13.
- M14.** Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R14.
- M15.** Each Generator Operator with a Blackstart Resource shall provide evidence, such as e-mails with receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within twenty-four hours of such changes in accordance with Requirement R15.
- M16.** Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R16.
- M17.** Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R17.
- M18.** Each Generator Operator shall have evidence, such as dated training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R18.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

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

The Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Approved restoration plan and any restoration plans in force since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of an updated restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three years for Requirement R4, Measure M4.
- The current, restoration plan approved by the Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- Implementation of its restoration plan or restoration plan strategies on any occasion for three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R7, Measure M7.
- Resynchronization of shut down areas on any occasion over three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R8, Measure M8.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R9, Measure M9.
- Actual training program materials or descriptions for three calendar years for Requirement R10, Measure M10.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit

as well as one previous compliance audit period for Requirement R12, Measure M12.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator, applicable Transmission Owner, and applicable Distribution provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Actual training program materials or descriptions and actual training records for three calendar years for Requirement R11, Measure M11.

If a Transmission Operator, applicable Transmission owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in force since its last compliance audit for Requirement R13, Measure M13.

The Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current documentation and any documentation in force since its last compliance audit on procedures to start each Blackstart Resources and for energizing a bus for Requirement R14, Measure M14.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R15, Measure M15.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R16, Measure M16.
- Actual training program materials and actual training records for three calendar years for Requirement R17, Measure M17.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Generator Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R18, Measure M18.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

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

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Transmission Operator has an approved plan but failed to comply with one of the sub-requirements within the requirement.	The Transmission Operator has an approved plan but failed to comply with two of the sub-requirements within the requirement.	The Transmission Operator has an approved plan but failed to comply with three of the sub-requirements within the requirement.	The Transmission Operator does not have an approved restoration plan.
R2.	The Transmission Operator failed to provide one of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was up to 10 calendar days late in doing so.	The Transmission Operator failed to provide two of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was more than 10 and less than or equal to 20 calendar days late in doing so.	The Transmission Operator failed to provide three of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was more than 20 and less than or equal to 30 calendar days late in doing so.	The Transmission Operator failed to provide four or more of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was more than 30 calendar days late in doing so.
R3.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change within 30 calendar days after the pre-determined schedule.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change more than 30 and less than or equal to 60 calendar days after the pre-determined schedule.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change more than 60 and less than or equal to 90 calendar days after the pre-determined schedule.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change more than 90 calendar days after the pre-determined schedule.
R4.	The Transmission Operator failed to update and submit its restoration plan to the	The Transmission Operator failed to update and submit its restoration plan to the	The Transmission Operator has failed to update and submit its restoration plan to the	The Transmission Operator has failed to update and submit its restoration plan to the

Standard EOP-005-2 — System Restoration from Blackstart Resources

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Reliability Coordinator within 90 calendar days of an unplanned change.	Reliability Coordinator within more than 90 calendar days but less than 120 calendar days of an unplanned change.	Reliability Coordinator within more than 120 calendar days but less than 150 calendar days of an unplanned change.	Reliability Coordinator within more than 150 calendar days of an unplanned change. OR The Transmission Operator failed to update and submit its restoration plan to the Reliability Coordinator prior to a planned BES modification.
R5.	N/A	N/A	N/A	The Transmission Operator did not make the latest Reliability Coordinator approved restoration plan available in its primary and backup control rooms prior to its implementation date.
R6.	The Transmission Operator performed the verification within the required timeframe but did not comply with one of the sub-requirements.	The Transmission Operator performed the verification within the required timeframe but did not comply with two of the sub-requirements.	The Transmission Operator performed the verification but did not complete it within the five calendar year period.	The Transmission Operator did not perform the verification or it took more than six calendar years to complete the verification. OR The Transmission Operator performed the verification within the required timeframe but did not comply with any of the sub-requirements.
R7.	N/A	N/A	N/A	The Transmission Operator did not implement its restoration plan following a Disturbance in which Blackstart Resources have been utilized in restoring

Standard EOP-005-2 — System Restoration from Blackstart Resources

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				the shut down area of the BES. Or, if the restoration plan cannot be executed as expected, the Transmission Operator did not utilize its restoration plan strategies to facilitate restoration.
R8.	N/A	N/A	N/A	The Transmission Operator resynchronized without approval of the Reliability Coordinator or not in accordance with the established procedures of the Reliability Coordinator following a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service.
R9.	N/A	N/A	N/A	The Transmission Operator's Blackstart Resource testing requirements do not address one or more of the sub-requirements of Requirement R9.
R10.	The Transmission Operator's training does not address one of the sub-requirements of Requirement R10.	The Transmission Operator's training does not address two of the sub-requirements of Requirement R10.	The Transmission Operator's training does not address three or more of the sub-requirements of Requirement R10.	The Transmission Operator has not included System restoration training in its operations training program.
R11.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train 5% or less of the personnel required by	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 5% and up to 10% of the	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 10% and up to 15% of the	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider failed to train more than 15% of the personnel

Standard EOP-005-2 — System Restoration from Blackstart Resources

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R11 within a two calendar year period.	personnel required by Requirement R11 within a two calendar year period.	personnel required by Requirement R11 within a two calendar year period.	required by Requirement R11 within a two calendar year period.
R12.	N/A.	N/A	N/A	The Transmission Operator has failed to comply with a request for their participation from the Reliability Coordinator.
R13.	N/A	The Transmission Operator and Generator Operator with a Blackstart Resource do not reference Blackstart Resource Testing requirements in their written Blackstart Resource Agreements or mutually agreed upon procedures or protocols.	N/A	The Transmission Operator and Generator Operator with a Blackstart resource do not have a written Blackstart Resource Agreement or mutually agreed upon procedure or protocol.
R14.	N/A	N/A	N/A	The Generator Operator does not have documented starting and bus energizing procedures for each Blackstart Resource.
R15.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator’s restoration plan within 24 hours but did make the notification within 48 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator’s restoration plan within 48 hours but did make the notification within 72 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator’s restoration plan within 72 hours but did make the notification within 96 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a known change in Blackstart Resource capability affecting the ability to meet the Transmission Operator’s restoration plan for more than 96 hours.
R16.	The GOP with a Blackstart Resource performed tests and	The GOP with a Blackstart Resource performed tests and	The GOP with a Blackstart Resource performed tests but	The Generator Operator with a Blackstart Resource did not

Standard EOP-005-2 — System Restoration from Blackstart Resources

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>maintained records but the records did not include all of the items in R16.1. OR The Generator Operator did not supply the Blackstart Resource testing records as requested for 31 to 60 calendar days of the request.</p>	<p>maintained records but did not supply the Blackstart Resource testing records as requested for 61 days to 90 calendar days after the request.</p>	<p>either did not maintain records or did not supply the Blackstart Resource testing records as requested within 91 or more calendar days after the request.</p>	<p>perform Blackstart Resource tests.</p>
R17.	<p>The Generator Operator with a Blackstart Resource did not train less than or equal to 10% of the personnel required by Requirement R17 within a two calendar year period.</p>	<p>The Generator Operator with a Blackstart Resource did not train more than 10% and less than or equal to 25% of the personnel required by Requirement R17 within a two calendar year period.</p>	<p>The Generator Operator with a Blackstart Resource did not train more than 25% and less than or equal to 50% of the personnel required by Requirement R17 within a two calendar year period.</p>	<p>The Generator Operator with a Blackstart Resource did not train more than 50% of the personnel required by Requirement R17 within a two calendar year period.</p>
R18.	<p>N/A.</p>	<p>N/A</p>	<p>N/A</p>	<p>The Generator Operator failed to participate in the Reliability Coordinator’s restoration drills, exercises, or simulations as requested by the Reliability Coordinator.</p>

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	May 2, 2007	Approved by Board of Trustees	Revised
2	TBD	Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-005-2 (approval effective 5/23/11)	
2	February 7, 2013	R3.1 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	July 1, 2013	Updated VRFs and VSLs based on June 24, 2013 approval.	
2	November 21, 2013	R3.1 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard EOP-005-2 — System Restoration from Blackstart Resources

United States

Standard	Requirement	Enforcement Date	Inactive Date
EOP-005-2	R1.	07/01/2013	
EOP-005-2	R1.1.	07/01/2013	
EOP-005-2	R1.2.	07/01/2013	
EOP-005-2	R1.3.	07/01/2013	
EOP-005-2	R1.4.	07/01/2013	
EOP-005-2	R1.5.	07/01/2013	
EOP-005-2	R1.6.	07/01/2013	
EOP-005-2	R1.7.	07/01/2013	
EOP-005-2	R1.8.	07/01/2013	
EOP-005-2	R1.9.	07/01/2013	
EOP-005-2	R2.	07/01/2013	
EOP-005-2	R3.	07/01/2013	
EOP-005-2	R3.1.	07/01/2013	01/21/2014
EOP-005-2	R4.	07/01/2013	
EOP-005-2	R4.1.	07/01/2013	
EOP-005-2	R5.	07/01/2013	
EOP-005-2	R6.	07/01/2013	
EOP-005-2	R6.1.	07/01/2013	
EOP-005-2	R6.2.	07/01/2013	
EOP-005-2	R6.3.	07/01/2013	
EOP-005-2	R7.	07/01/2013	
EOP-005-2	R8.	07/01/2013	
EOP-005-2	R9.	07/01/2013	
EOP-005-2	R9.1.	07/01/2013	
EOP-005-2	R9.2.	07/01/2013	
EOP-005-2	R9.2.1.	07/01/2013	
EOP-005-2	R9.2.2.	07/01/2013	
EOP-005-2	R9.3.	07/01/2013	
EOP-005-2	R10.	07/01/2013	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard EOP-005-2 — System Restoration from Blackstart Resources

United States

EOP-005-2	R10.1.	07/01/2013	
EOP-005-2	R10.2.	07/01/2013	
EOP-005-2	R10.3.	07/01/2013	
EOP-005-2	R10.4.	07/01/2013	
EOP-005-2	R11.	07/01/2013	
EOP-005-2	R12.	07/01/2013	
EOP-005-2	R13.	07/01/2013	
EOP-005-2	R14.	07/01/2013	
EOP-005-2	R15.	07/01/2013	
EOP-005-2	R16.	07/01/2013	
EOP-005-2	R16.1.	07/01/2013	
EOP-005-2	R16.2.	07/01/2013	
EOP-005-2	R17.	07/01/2013	
EOP-005-2	R17.1.	07/01/2013	
EOP-005-2	R17.2.	07/01/2013	
EOP-005-2	R18.	07/01/2013	

A. Introduction

1. **Title:** Coordination of Plans For New Generation, Transmission, and End-User Facilities
2. **Number:** FAC-002-1
3. **Purpose:** To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.
4. **Applicability:**
 - 4.1. Generator Owner
 - 4.2. Transmission Owner
 - 4.3. Distribution Provider
 - 4.4. Load-Serving Entity
 - 4.5. Transmission Planner
 - 4.6. Planning Authority
5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

- R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:
 - 1.1. Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.
 - 1.2. Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.
 - 1.3. Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.
 - 1.4. Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.
 - 1.5. Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.
- R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional

Reliability Organization(s) and NERC on request (within 30 calendar days). (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider’s documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.
- M2.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process

- 1.1. Compliance Enforcement Authority**
Regional Entity.
- 1.2. Compliance Monitoring Period and Reset Timeframe**
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**
Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.
- 1.5. Additional Compliance Information**
None

2. Violation Severity Levels (no changes)

E. Regional Differences

- 1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of “Regional Reliability Organizations(s).	Errata
1	August 5, 2010	Modified to address Order No. 693 Directives	Revised.

Standard FAC-002-1 — Coordination of Plans for New Facilities

		contained in paragraph 693. Adopted by the NERC Board of Trustees.	
1	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
1	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard FAC-002-1 — Coordination of Plans For New Generation, Transmission, and End-User Facilities

United States

Standard	Requirement	Enforcement Date	Inactive Date
FAC-002-1	R1.	10/01/2011	
FAC-002-1	R1.1.	10/01/2011	
FAC-002-1	R1.2.	10/01/2011	
FAC-002-1	R1.3.	10/01/2011	
FAC-002-1	R1.4.	10/01/2011	
FAC-002-1	R1.5.	10/01/2011	
FAC-002-1	R2.	10/01/2011	01/21/2014

A. Introduction

1. **Title:** Facility Ratings
2. **Number:** FAC-008-3
3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.
4. **Applicability**
 - 4.1. Transmission Owner.
 - 4.2. Generator Owner.
5. **Effective Date:** The first day of the first calendar quarter that is twelve months beyond the date approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter twelve months following BOT adoption.

B. Requirements

- R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. [*Violation Risk Factor: Lower*] [*Time Horizon: Long-term Planning*]
 - 1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:
 - Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
 - Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.
 - 1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
- R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. [*Violation Risk Factor: Medium*] [*Time Horizon: Long-term Planning*]
 - 2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:
 - Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
 - A practice that has been verified by testing, performance history or engineering analysis.
- 2.2.** The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:
- 2.2.1.** Equipment Rating standard(s) used in development of this methodology.
 - 2.2.2.** Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
 - 2.2.3.** Ambient conditions (for particular or average conditions or as they vary in real-time).
 - 2.2.4.** Operating limitations.¹
- 2.3.** A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
- 2.4.** The process by which the Rating of equipment that comprises a Facility is determined.
- 2.4.1.** The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
 - 2.4.2.** The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.
- R3.** Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*
- 3.1.** The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:
 - Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
 - One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
 - A practice that has been verified by testing, performance history or engineering analysis.
 - 3.2.** The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:
 - 3.2.1.** Equipment Rating standard(s) used in development of this methodology.

¹ Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

- 3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
 - 3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).
 - 3.2.4. Operating limitations.²
 - 3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
 - 3.4. The process by which the Rating of equipment that comprises a Facility is determined.
 - 3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
 - 3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.
- R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retirement approved by FERC effective January 21, 2014.)
- R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retirement approved by FERC effective January 21, 2014.)
- R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- R7. Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s),

² Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- 8.1.** As scheduled by the requesting entities:
 - 8.1.1.** Facility Ratings
 - 8.1.2.** Identity of the most limiting equipment of the Facilities
- 8.2.** Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:
 - 8.2.1.** Identity of the existing next most limiting equipment of the Facility
 - 8.2.2.** The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

C. Measures

- M1.** Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.
- M2.** Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.
- M3.** Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.
- M4.** Each Transmission Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement 4. The Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its documentation for determining its Facility Ratings or its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement R4. (Retirement approved by NERC BOT pending applicable regulatory approval.)
- M5.** If the Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology or a Generator Owner's documentation for determining its Facility Ratings, the Transmission Owner or Generator Owner shall have evidence, (such as a copy of a dated electronic or hard copy note, or other comparable evidence from the Transmission Owner or Generator Owner addressed to the commenter that includes the response to the comment,) that it provided a response to that commenting entity in accordance with Requirement R5. (Retirement approved by NERC BOT pending applicable regulatory approval.)
- M6.** Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).
- M7.** Each Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings to its associated Reliability

Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R7.

- M8.** Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Compliance Monitoring and Enforcement Processes:

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting
- Compliance Violation Investigations
- Complaints

1.3. Data Retention

The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.

The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.

The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.

The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.

The Generator Owner and Transmission Owner shall each keep evidence for Measure M4, and Measure M5, for three calendar years. (Retirement approved by FERC effective January 21, 2014.)

The Generator Owner shall keep evidence for Measure M7 for three calendar years.

The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.

If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.

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

1.4. Additional Compliance Information

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	<ul style="list-style-type: none"> • The Generator Owner’s Facility Rating documentation did not address Requirement R1, Part 1.1. 	The Generator Owner’s Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2	<p>The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4 	<p>The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4 	<p>The Generator Owner’s Facility Rating methodology did not address all the components of Requirement R2, Part 2.4.</p> <p>OR</p> <p>The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4 	<p>The Generator Owner’s Facility Rating methodology failed to recognize a facility’s rating based on the most limiting component rating as required in Requirement R2, Part 2.3</p> <p>OR</p> <p>The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
R3	<p>The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> • 3.1 • 3.2.1 	<p>The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> • 3.1 • 3.2.1 	<p>The Transmission Owner’s Facility Rating methodology did not address either of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> • 3.4.1 • 3.4.2 	<p>The Transmission Owner’s Facility Rating methodology failed to recognize a Facility’s rating based on the most limiting component rating as required in Requirement R3, Part 3.3</p> <p>OR</p>

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<ul style="list-style-type: none"> • 3.2.2 • 3.2.3 • 3.2.4 	<ul style="list-style-type: none"> • 3.2.2 • 3.2.3 • 3.2.4 	<p>OR</p> <p>The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4 	<p>The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
<p>R4</p> <p>(Retirement approved by FERC effective January 21, 2014.)</p>	<p>The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.</p>	<p>The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.</p>	<p>The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.</p>	<p>The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)</p>
<p>R5</p> <p>(Retirement approved by FERC effective January 21, 2014.)</p>	<p>The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)</p>	<p>The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request.</p> <p>OR</p> <p>The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)</p>	<p>The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request.</p> <p>OR</p> <p>The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation. (R5)</p>	<p>The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)</p>

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 15% of its solely owned and jointly owned Facilities. (R6)
R7	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the requesting entities.
R8	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but the information	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more

Standard FAC-008-3 — Facility Ratings

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>was provided up to and including 15 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)</p>	<p>The responsible entity provided the required Rating information to the requesting entity, but did so more than 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)</p>	<p>The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)</p>	<p>than 35 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)</p>

E. Regional Variances

None.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	
3	February 7, 2013	R4 and R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
3	November 21, 2013	R4 and R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard FAC-008-3 — Facility Ratings

United States

Standard	Requirement	Enforcement Date	Inactive Date
FAC-008-3	R1.	01/01/2013	
FAC-008-3	R2.	01/01/2013	
FAC-008-3	R3.	01/01/2013	
FAC-008-3	R4.	01/01/2013	01/21/2014
FAC-008-3	R5.	01/01/2013	01/21/2014
FAC-008-3	R6.	01/01/2013	
FAC-008-3	R7.	01/01/2013	
FAC-008-3	R8.	01/01/2013	

A. Introduction

- 1. Title:** System Operating Limits Methodology for the Planning Horizon
- 2. Number:** FAC-010-2.1
- 3. Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable planning of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.
- 4. Applicability**
 - 4.1. Planning Authority**
- 5. Effective Date:** April 19, 2010

B. Requirements

- R1.** The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:
 - R1.1.** Be applicable for developing SOLs used in the planning horizon.
 - R1.2.** State that SOLs shall not exceed associated Facility Ratings.
 - R1.3.** Include a description of how to identify the subset of SOLs that qualify as IROLs.
- R2.** The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:
 - R2.1.** In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.
 - R2.2.** Following the single Contingencies¹ identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.
 - R2.2.1.** Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
 - R2.2.2.** Loss of any generator, line, transformer, or shunt device without a Fault.
 - R2.2.3.** Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
 - R2.3.** Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:
 - R2.3.1.** Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

¹ The Contingencies identified in R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

- M2.** The Planning Authority shall have evidence it issued its SOL Methodology and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Planning Authority that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Planning Authority shall self-certify its compliance to the Compliance Monitor at least once every three years. New Planning Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Planning Authority shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years.~~ In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired-Retirement approved by FERC effective January 21, 2014.)

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Planning Authority shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retirement approved by FERC effective January 21, 2014.)

1.4.2 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.3 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

- 2.1.2** No evidence of responses to a recipient's comments on the SOL Methodology.
(Retirement approved by FERC effective January 21, 2014.)
- 2.2. Level 2:** The SOL Methodology did not include a requirement to address all of the elements in R2.1 through R2.3 and E1.
- 2.3. Level 3:** There shall be a level three non-compliance if any of the following conditions exists:
 - 2.3.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.
 - 2.3.2** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.
 - 2.3.3** The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.
- 2.4. Level 4:** The SOL Methodology was not issued to all required entities in accordance with R4

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.2	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
R2	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 –R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
R3	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
R4	One or both of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority failed to issue its SOL Methodology and

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

Requirement	Lower	Moderate	High	Severe
	<p>to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but</p>

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

Requirement	Lower	Moderate	High	Severe
				four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
<p>R5 (Retirement approved by FERC effective January 21, 2014.)</p>	<p>The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.</p>	<p>The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.</p>	<p>The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days.</p> <p>OR</p> <p>The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.</p>	<p>The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer.</p> <p>OR</p> <p>The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.</p>

E. Regional Differences

- 1.** The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:
 - 1.1.** As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:
 - 1.1.1** Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.
 - 1.1.2** A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7
 - 1.1.3** Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.
 - 1.1.4** The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.
 - 1.1.5** A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.
 - 1.1.6** A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-010.
 - 1.1.7** The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.
 - 1.2.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:
 - 1.2.1** All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.
 - 1.2.2** Cascading does not occur.
 - 1.2.3** Uncontrolled separation of the system does not occur.
 - 1.2.4** The system demonstrates transient, dynamic and voltage stability.
 - 1.2.5** Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.
 - 1.2.6** Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

- 1.2.7** To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.
- 1.3.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:
- 1.3.1** Cascading does not occur.
- 1.4.** The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
1	November 1, 2006	Fixed typo. Removed the word “each” from the 1 st sentence of section D.1.3, Data Retention.	01/11/07
2	June 24, 2008	Adopted by Board of Trustees; FERC Order 705	Revised
2		Changed the effective date to July 1, 2008 Changed “Cascading Outage” to “Cascading” Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2.1	November 5, 2009	Adopted by the Board of Trustees — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	April 19, 2010	FERC Approved — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	February 7, 2013	R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

2.1	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	
-----	----------------------	--	--

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

United States

Standard	Requirement	Enforcement Date	Inactive Date
FAC-010-2.1	R1.	04/19/2010	
FAC-010-2.1	R1.1.	04/19/2010	
FAC-010-2.1	R1.2.	04/19/2010	
FAC-010-2.1	R1.3.	04/19/2010	
FAC-010-2.1	R2.	04/19/2010	
FAC-010-2.1	R2.1.	04/19/2010	
FAC-010-2.1	R2.2.	04/19/2010	
FAC-010-2.1	R2.2.1.	04/19/2010	
FAC-010-2.1	R2.2.2.	04/19/2010	
FAC-010-2.1	R2.2.3.	04/19/2010	
FAC-010-2.1	R2.3.	04/19/2010	
FAC-010-2.1	R2.3.1.	04/19/2010	
FAC-010-2.1	R2.3.2.	04/19/2010	
FAC-010-2.1	R2.4.	04/19/2010	
FAC-010-2.1	R2.5.	04/19/2010	
FAC-010-2.1	R2.6.	04/19/2010	
FAC-010-2.1	R2.6.1.	04/19/2010	
FAC-010-2.1	R3.	04/19/2010	
FAC-010-2.1	R3.1.	04/19/2010	
FAC-010-2.1	R3.2.	04/19/2010	
FAC-010-2.1	R3.3.	04/19/2010	
FAC-010-2.1	R3.4.	04/19/2010	
FAC-010-2.1	R3.5.	04/19/2010	
FAC-010-2.1	R3.6.	04/19/2010	
FAC-010-2.1	R4.	04/19/2010	
FAC-010-2.1	R4.1.	04/19/2010	
FAC-010-2.1	R4.2.	04/19/2010	
FAC-010-2.1	R4.3.	04/19/2010	
FAC-010-2.1	R5.	04/19/2010	01/21/2014

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

United States

A. Introduction

1. **Title:** System Operating Limits Methodology for the Operations Horizon
2. **Number:** FAC-011-2
3. **Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.
4. **Applicability**
 - 4.1. Reliability Coordinator
5. **Effective Date:** April 29, 2009

B. Requirements

- R1. The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:
 - R1.1. Be applicable for developing SOLs used in the operations horizon.
 - R1.2. State that SOLs shall not exceed associated Facility Ratings.
 - R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.
- R2. The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:
 - R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.
 - R2.2. Following the single Contingencies¹ identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.
 - R2.2.1. Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
 - R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.
 - R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
 - R2.3. In determining the system's response to a single Contingency, the following shall be acceptable:
 - R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

¹ The Contingencies identified in FAC-011 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

C. Measures

- M1.** The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.
- M2.** The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.
- M3.** If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Reliability Coordinator that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years.~~ In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired-Retirement approved by FERC effective January 21, 2014.)

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses.
(Retirement approved by FERC effective January 21, 2014.)

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
R4	One or both of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	<p>provided up to 30 calendar days after the effectiveness of the change.</p>	<p>calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to</p>

Standard FAC-011-2 — System Operating Limits Methodology for the Operations Horizon

Requirement	Lower	Moderate	High	Severe
<p>R5 (Retirement approved by FERC effective January 21, 2014.)</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.</p>	<p>30 calendar days after the effectiveness of the change. The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.</p>

Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:
 - 1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:
 - 1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.
 - 1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7
 - 1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.
 - 1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.
 - 1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.
 - 1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.
 - 1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.
 - 1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:
 - 1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.
 - 1.2.2 Cascading does not occur.
 - 1.2.3 Uncontrolled separation of the system does not occur.
 - 1.2.4 The system demonstrates transient, dynamic and voltage stability.
 - 1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.
 - 1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

- 1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.
- 1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:
 - 1.3.1 Cascading does not occur.
- 1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed “Cascading Outage” to “Cascading” Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	February 7, 2013	R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard FAC-011-2 — System Operating Limits Methodology for the Operations Horizon

United States

Standard	Requirement	Enforcement Date	Inactive Date
FAC-011-2	R1.	04/29/2009	
FAC-011-2	R1.1.	04/29/2009	
FAC-011-2	R1.2.	04/29/2009	
FAC-011-2	R1.3.	04/29/2009	
FAC-011-2	R2.	04/29/2009	
FAC-011-2	R2.1.	04/29/2009	
FAC-011-2	R2.2.	04/29/2009	
FAC-011-2	R2.2.1.	04/29/2009	
FAC-011-2	R2.2.2.	04/29/2009	
FAC-011-2	R2.2.3.	04/29/2009	
FAC-011-2	R2.3.	04/29/2009	
FAC-011-2	R2.3.1.	04/29/2009	
FAC-011-2	R2.3.2.	04/29/2009	
FAC-011-2	R2.3.3.	04/29/2009	
FAC-011-2	R2.4.	04/29/2009	
FAC-011-2	R3.	04/29/2009	
FAC-011-2	R3.1.	04/29/2009	
FAC-011-2	R3.2.	04/29/2009	
FAC-011-2	R3.3.	04/29/2009	
FAC-011-2	R3.3.1.	04/29/2009	
FAC-011-2	R3.4.	04/29/2009	
FAC-011-2	R3.5.	04/29/2009	
FAC-011-2	R3.6.	04/29/2009	
FAC-011-2	R3.7.	04/29/2009	
FAC-011-2	R4.	04/29/2009	
FAC-011-2	R4.1.	04/29/2009	
FAC-011-2	R4.2.	04/29/2009	
FAC-011-2	R4.3.	04/29/2009	
FAC-011-2	R5.	04/29/2009	01/21/2014

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard FAC-011-2 — System Operating Limits Methodology for the Operations Horizon

United States

A. Introduction

- 1. Title:** Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon
- 2. Number:** FAC-013-2
- 3. Purpose:** To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.
- 4. Applicability:**
 - 4.1. Planning Coordinators**
- 5. Effective Date:**

In those jurisdictions where regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after applicable regulatory approval or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-2 are effective.

In those jurisdictions where no regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after Board of Trustees adoption or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1 and MOD-030-2 are effective.

B. Requirements

- R1.** Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: [*Violation Risk Factor: Medium*] [*Time Horizon: Long-term Planning*]
 - 1.1.** Criteria for the selection of the transfers to be assessed.
 - 1.2.** A statement that the assessment shall respect known System Operating Limits (SOLs).
 - 1.3.** A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's planning practices.
 - 1.4.** A description of how each of the following assumptions and criteria used in performing the assessment are addressed:
 - 1.4.1.** Generation dispatch, including but not limited to long term planned outages, additions and retirements.
 - 1.4.2.** Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.
 - 1.4.3.** System demand.
 - 1.4.4.** Current approved and projected Transmission uses.

Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

- 1.4.5. Parallel path (loop flow) adjustments.
 - 1.4.6. Contingencies
 - 1.4.7. Monitored Facilities.
- 1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.
- R2.** Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*
 - 2.1. Distribute to the following prior to the effectiveness of such revisions:
 - 2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.
 - 2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.
 - 2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.
- R3.** If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]*
(Retirement approved by FERC effective January 21, 2014.)
- R4.** During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*
- R5.** Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*
- R6.** If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area

Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

C. Measures

- M1.** Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.
- M2.** Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2
- Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. **(Retirement approved by FERC effective January 21, 2014.)**
- M3.** Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.
- M4.** Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5.
- M5.** Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Data Retention

The Planning Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. **(R3 retired- Retirement approved by FERC effective January 21, 2014.)**

Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	<p>The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.</p>	<p>The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology:</p> <ul style="list-style-type: none"> • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.</p>	<p>The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology:</p> <ul style="list-style-type: none"> • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.</p>	<p>The Planning Coordinator did not have a Transfer Capability methodology.</p> <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology:</p> <ul style="list-style-type: none"> • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.</p>

Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

<p>R2</p>	<p>The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.</p>	<p>The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request</p>	<p>The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.</p>	<p>The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.</p>
<p>R3 (Retirement approved by FERC effective January 21, 2013.)</p>	<p>The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.</p>	<p>The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.</p>	<p>The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.</p>	<p>The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern.</p> <p>OR</p> <p>The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.</p>

Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

R4	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.
----	---	--	--	--

Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

R5	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.

Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

E. Regional Variances

None.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	08/01/05	<ol style="list-style-type: none"> 1. Changed incorrect use of certain hyphens (-) to “en dash (–).” 2. Lower cased the word “draft” and “drafting team” where appropriate. 3. Changed Anticipated Action #5, page 1, from “30-day” to “Thirty-day.” 4. Added or removed “periods.” 	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	05/17/12	<p>FERC Order issued directing the VRF’s for Requirements R1. and R4. be changed from “Lower” to “Medium.”</p> <p>FERC Order issued correcting the High and Severe VSL language for R1.</p>	
2	02/7/13	R3 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	11/21/13	R3 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard FAC-013-2 — Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

United States

Standard	Requirement	Enforcement Date	Inactive Date
FAC-013-2	R1.	04/01/2013	
FAC-013-2	R2.	04/01/2013	
FAC-013-2	R3.	04/01/2013	01/21/2014
FAC-013-2	R4.	04/01/2013	
FAC-013-2	R5.	04/01/2013	
FAC-013-2	R6.	04/01/2013	

A. Introduction

1. **Title:** Interchange Confirmation
2. **Number:** INT-007-1
3. **Purpose:** To ensure that each Arranged Interchange is checked for reliability before it is implemented.
4. **Applicability**
 - 4.1. Interchange Authority.
5. **Effective Date:** January 1, 2007

B. Requirements

- R1. The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:
 - R1.1. Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).
 - R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry. (Retirement approved by FERC effective January 21, 2014.)
 - R1.3. The following are defined:
 - R1.3.1. Generation source and load sink.
 - R1.3.2. Megawatt profile.
 - R1.3.3. Ramp start and stop times.
 - R1.3.4. Interchange duration.
 - R1.4. Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.

C. Measures

- M1. For each Arranged Interchange, the Interchange Authority shall show evidence that it has verified the Arranged Interchange information prior to the dissemination of the Confirmed Interchange.

D. Compliance

1. **Compliance Monitoring Process**
 - 1.1. **Compliance Monitoring Responsibility**

Regional Reliability Organization.
 - 1.2. **Compliance Monitoring Period and Reset Time Frame**

The Performance-Reset Period shall be twelve months from the last noncompliance to Requirement 1.
 - 1.3. **Data Retention**

The Interchange Authority shall keep 90 days of historical data. The Compliance Monitor shall keep audit records for a minimum of three calendar years.

1.4. Additional Compliance Information

Each Interchange Authority shall demonstrate compliance to the Compliance Monitor within the first year that this standard becomes effective or the first year the entity commences operation by self-certification to the Compliance Monitor.

Subsequent to the initial compliance review, compliance may be:

- 1.4.1 Verified by audit at least once every three years.
- 1.4.2 Verified by spot checks in years between audits.
- 1.4.3 Verified by annual audits of noncompliant Interchange Authorities, until compliance is demonstrated.
- 1.4.4 Verified at any time as the result of a complaint. Complaints must be lodged within 60 days of the incident. Complaints will be evaluated by the Compliance Monitor.

Each Interchange Authority shall make the following available for inspection by the Compliance Monitor upon request:

- 1.4.5 For compliance audits and spot checks, relevant data and system log records for the audit period which indicate an Interchange Authority's verification that all Arranged Interchange was balanced and valid as defined in R1. The Compliance Monitor may request up to a three-month period of historical data ending with the date the request is received by the Interchange Authority.
- 1.4.6 For specific complaints, only those data and system log records associated with the specific Interchange event contained in the complaint which indicate an Interchange Authority's verification that an Arranged Interchange was balanced and valid as defined in R1 for that specific Interchange

2. Levels of Non-Compliance

- 2.1. **Level 1:** One occurrence¹ where Interchange-related data was not verified as defined in R1.
- 2.2. **Level 2:** Two occurrences where Interchange-related data was not verified as defined in R1.
- 2.3. **Level 3:** Three occurrences where Interchange-related data was not verified as defined in R1.
- 2.4. **Level 4:** Four or more occurrences where Interchange-related data was not verified as defined in R1.

E. Regional Differences

None

¹ This does not include instances of not verifying due to extenuating circumstances approved by the Compliance Monitor.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by the NERC Board of Trustees	
1	March 16, 2007	FERC Approved	
1	February 7, 2013	R1.2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
1	November 21, 2013	R1.2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard INT-007-1 — Interchange Confirmation

United States

Standard	Requirement	Enforcement Date	Inactive Date
INT-007-1	R1.	06/18/2007	
INT-007-1	R1.1.	06/18/2007	
INT-007-1	R1.2.	06/18/2007	01/21/2014
INT-007-1	R1.3.	06/18/2007	
INT-007-1	R1.3.1.	06/18/2007	
INT-007-1	R1.3.2.	06/18/2007	
INT-007-1	R1.3.3.	06/18/2007	
INT-007-1	R1.3.4.	06/18/2007	
INT-007-1	R1.4.	06/18/2007	

A. Introduction

- 1. Title:** Coordination of Real-time Activities Between Reliability Coordinators
- 2. Number:** IRO-016-1
- 3. Purpose:** To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.
- 4. Applicability**
 - 4.1. Reliability Coordinator**
- 5. Effective Date:** November 1, 2006

B. Requirements

- R1.** The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
 - R1.1.** If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.
 - R1.2.** If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
 - R1.2.1.** If time permits, this re-evaluation shall be done before taking corrective actions.
 - R1.2.2.** If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.
 - R1.3.** If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.
- R2.** The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.
(Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1.** For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

D. Compliance

- 1. Compliance Monitoring Process**
 - 1.1. Compliance Monitoring Responsibility**

Regional Reliability Organization
 - 1.2. Compliance Monitoring Period and Reset Time Frame**

The performance reset period shall be one calendar year.

1.3. Data Retention

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

1.4. Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction’s discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

- 1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

2. Levels of Non-Compliance

- 2.1. **Level 1:** For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.
- 2.2. **Level 2:** Not applicable.
- 2.3. **Level 3:** Not applicable.
- 2.4. **Level 4:** For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to “en dash (–).” 2. Hyphenated “30-day” and “Reliability Coordinator-to-Reliability Coordinator” when used as adjective.	01/20/06

Standard IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators

		<ol style="list-style-type: none"> 3. Changed standard header to be consistent with standard “Title.” 4. Added “periods” to items where appropriate. 5. Initial capped heading “Definitions of Terms Used in Standard.” 6. Changed “Timeframe” to “Time Frame” in item D, 1.2. 7. Lower cased all words that are not “defined” terms — drafting team, and self-certification. 8. Changed apostrophes to “smart” symbols. 9. Removed comma after word “condition” in item R.1.1. 10. Added comma after word “expected” in item 1.4, last sentence. 11. Removed extra spaces between words where appropriate. 	
1	February 7, 2006	Adopted by NERC Board of Trustees	
1	March 16, 2007	Approved by FERC	
1	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
1	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators

United States

Standard	Requirement	Enforcement Date	Inactive Date
IRO-016-1	R1.	06/18/2007	
IRO-016-1	R1.1.	06/18/2007	
IRO-016-1	R1.2.	06/18/2007	
IRO-016-1	R1.2.1.	06/18/2007	
IRO-016-1	R1.2.2.	06/18/2007	
IRO-016-1	R1.3.	06/18/2007	
IRO-016-1	R2.	06/18/2007	01/21/2014

A. Introduction

1. **Title:** Nuclear Plant Interface Coordination
2. **Number:** NUC-001-2
3. **Purpose:** This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.
4. **Applicability:**
 - 4.1. Nuclear Plant Generator Operator.
 - 4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:
 - 4.2.1 Transmission Operators.
 - 4.2.2 Transmission Owners.
 - 4.2.3 Transmission Planners.
 - 4.2.4 Transmission Service Providers.
 - 4.2.5 Balancing Authorities.
 - 4.2.6 Reliability Coordinators.
 - 4.2.7 Planning Coordinators.
 - 4.2.8 Distribution Providers.
 - 4.2.9 Load-serving Entities.
 - 4.2.10 Generator Owners.
 - 4.2.11 Generator Operators.
5. **Effective Date:** April 1, 2010

B. Requirements

- R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]
- R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements¹ that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Medium*]
- R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]
- R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

- R4.1.** Incorporate the NPIRs into their operating analyses of the electric system.
- R4.2.** Operate the electric system to meet the NPIRs.
- R4.3.** Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.
- R5.** The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]
- R6.** Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]
- R7.** Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]
- R8.** Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]
- R9.** The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]
 - R9.1.** Administrative elements: (Retirement approved by FERC effective January 21, 2014.)
 - R9.1.1.** Definitions of key terms used in the agreement. (Retirement approved by FERC effective January 21, 2014.)
 - R9.1.2.** Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. (Retirement approved by FERC effective January 21, 2014.)
 - R9.1.3.** A requirement to review the agreement(s) at least every three years. (Retirement approved by FERC effective January 21, 2014.)
 - R9.1.4.** A dispute resolution mechanism. (Retirement approved by effective January 21, 2014.)
 - R9.2.** Technical requirements and analysis:
 - R9.2.1.** Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.
 - R9.2.2.** Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.
 - R9.2.3.** Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.
 - R9.3.** Operations and maintenance coordination:

- R9.3.1.** Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.
- R9.3.2.** Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.
- R9.3.3.** Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.
- R9.3.4.** Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.
- R9.3.5.** Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. .
- R9.3.6.** Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.
- R9.3.7.** Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.
- R9.4.** Communications and training:
 - R9.4.1.** Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.
 - R9.4.2.** Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.
 - R9.4.3.** Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.
 - R9.4.4.** Provisions for supplying information necessary to report to government agencies, as related to NPIRs.
 - R9.4.5.** Provisions for personnel training, as related to NPIRs.

C. Measures

- M1.** The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)
- M2.** The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. (Requirement 2 and 9)

- M3.** Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)
- M4.** Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:
 - M4.1** The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)
 - M4.2** The electric system was operated to meet the NPIRs. (Requirement 4.2)
 - M4.3** The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)
- M5.** The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)
- M6.** The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)
- M7.** The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)
- M8.** The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

D. Compliance

- 1. Compliance Monitoring Process**
 - 1.1. Compliance Enforcement Authority**
 - Regional Entity.
 - 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

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

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

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

- 2.1. Lower:** Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.
- 2.2. Moderate:** Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.
- 2.3. High:** One or more requirements of R3 through R8 were not met.
- 2.4. Severe:** No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

E. Regional Differences

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs.

Therefore the definition of NPLR for Canadian CANDU units will be as follows:

Nuclear Plant Licensing Requirements (NPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this

Standard NUC-001-2 — Nuclear Plant Interface Coordination

standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	Revision
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update
2	February 7, 2013	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2	November 21, 2013	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard NUC-001-2 — Nuclear Plant Interface Coordination

United States

Standard	Requirement	Enforcement Date	Inactive Date
NUC-001-2	R1.	04/01/2010	
NUC-001-2	R2.	04/01/2010	
NUC-001-2	R3.	04/01/2010	
NUC-001-2	R4.	04/01/2010	
NUC-001-2	R4.1.	04/01/2010	
NUC-001-2	R4.2.	04/01/2010	
NUC-001-2	R4.3.	04/01/2010	
NUC-001-2	R5.	04/01/2010	
NUC-001-2	R6.	04/01/2010	
NUC-001-2	R7.	04/01/2010	
NUC-001-2	R8.	04/01/2010	
NUC-001-2	R9.	04/01/2010	
NUC-001-2	R9.1.	04/01/2010	01/21/2014
NUC-001-2	R9.1.1.	04/01/2010	01/21/2014
NUC-001-2	R9.1.2.	04/01/2010	01/21/2014
NUC-001-2	R9.1.3.	04/01/2010	01/21/2014
NUC-001-2	R9.1.4.	04/01/2010	01/21/2014
NUC-001-2	R9.2.	04/01/2010	
NUC-001-2	R9.2.1.	04/01/2010	
NUC-001-2	R9.2.2.	04/01/2010	
NUC-001-2	R9.2.3.	04/01/2010	
NUC-001-2	R9.3.	04/01/2010	
NUC-001-2	R9.3.1.	04/01/2010	
NUC-001-2	R9.3.2.	04/01/2010	
NUC-001-2	R9.3.3.	04/01/2010	
NUC-001-2	R9.3.4.	04/01/2010	
NUC-001-2	R9.3.5.	04/01/2010	
NUC-001-2	R9.3.6.	04/01/2010	
NUC-001-2	R9.3.7.	04/01/2010	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard NUC-001-2 — Nuclear Plant Interface Coordination

United States

NUC-001-2	R9.4.	04/01/2010	
NUC-001-2	R9.4.1.	04/01/2010	
NUC-001-2	R9.4.2.	04/01/2010	
NUC-001-2	R9.4.3.	04/01/2010	
NUC-001-2	R9.4.4.	04/01/2010	
NUC-001-2	R9.4.5.	04/01/2010	

A. Introduction

1. **Title:** **Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.**
2. **Number:** PRC-010-0
3. **Purpose:** Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.
4. **Applicability:**
 - 4.1. Load-Serving Entity that operates a UVLS program
 - 4.2. Transmission Owner that owns a UVLS program
 - 4.3. Transmission Operator that operates a UVLS program
 - 4.4. Distribution Provider that owns or operates a UVLS program
5. **Effective Date:** April 1, 2005

B. Requirements

- R1.** The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).
- R1.1.** This assessment shall include, but is not limited to:
- R1.1.1.** Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.
 - R1.1.2.** Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.
 - R1.1.3.** A review of the voltage set points and timing.
- R2.** The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1.** Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0_R1.
- M2.** Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0_R2. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

1.2. Compliance Monitoring Period and Reset Timeframe

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0_R1.1 or an assessment of the UVLS program was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	February 8, 2005	Adopted by NERC Board of Trustees	
0	March 16, 2007	Approved by FERC	
0	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
0	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard PRC-010-0 — Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program

United States

Standard	Requirement	Enforcement Date	Inactive Date
PRC-010-0	R1.	06/18/2007	
PRC-010-0	R1.1.	06/18/2007	
PRC-010-0	R1.1.1.	06/18/2007	
PRC-010-0	R1.1.2.	06/18/2007	
PRC-010-0	R1.1.3.	06/18/2007	
PRC-010-0	R2.	06/18/2007	01/21/2014

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

A. Introduction

1. **Title:** Under-Voltage Load Shedding Program Performance
2. **Number:** PRC-022-1
3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).
4. **Applicability**
 - 4.1. Transmission Operator that operates a UVLS program.
 - 4.2. Distribution Provider that operates a UVLS program.
 - 4.3. Load-Serving Entity that operates a UVLS program.
5. **Effective Date:** May 1, 2006

B. Requirements

- R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:
 - R1.1. A description of the event including initiating conditions.
 - R1.2. A review of the UVLS set points and tripping times.
 - R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.
 - R1.4. A summary of the findings.
 - R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.
- R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. (Retirement approved by FERC effective January 21, 2014.)

C. Measures

- M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.
- M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization. (Retirement approved by FERC effective January 21, 2014.)

D. Compliance

1. Compliance Monitoring Process
 - 1.1. **Compliance Monitoring Responsibility**

Regional Reliability Organization.

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider 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.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

2.3. Level 3: Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

2.4. Level 4: Documentation of the analysis of UVLS performance was not provided.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	December 1, 2005	<ol style="list-style-type: none"> 1. Removed comma after 2004 in “Development Steps Completed,” #1. 2. Changed incorrect use of certain hyphens (-) to “en dash” (–) and “em dash (—).” 3. Lower cased the word “region,” “board,” and “regional” throughout document where appropriate. 4. Added or removed “periods” where appropriate. 5. Changed “Timeframe” to “Time Frame” in item D, 1.2. 	January 20, 2006
1	February 7, 2006	Adopted by the NERC Board of Trustees	
1	March 16, 2007	Approved by FERC	
1	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending	

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

		applicable regulatory approval.	
1	November 21, 2013	R2 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

United States

Standard	Requirement	Enforcement Date	Inactive Date
PRC-022-1	R1.	06/18/2007	
PRC-022-1	R1.1.	06/18/2007	
PRC-022-1	R1.2.	06/18/2007	
PRC-022-1	R1.3.	06/18/2007	
PRC-022-1	R1.4.	06/18/2007	
PRC-022-1	R1.5.	06/18/2007	
PRC-022-1	R2.	06/18/2007	01/21/2014

Standard VAR-001-2 — Voltage and Reactive Control

A. Introduction

1. **Title:** Voltage and Reactive Control
2. **Number:** VAR-001-2
3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.
4. **Applicability:**
 - 4.1. Transmission Operators.
 - 4.2. Purchasing-Selling Entities.
 - 4.3. Load Serving Entities.
5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

- R1.** Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.
- R2.** Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.
- R3.** The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.
 - R3.1.** Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.
 - R3.2.** For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.
- R4.** Each Transmission Operator shall specify a voltage or Reactive Power schedule ¹ at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).
- R5.** Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.
(Retirement approved by FERC effective January 21, 2014.)

¹ The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

Standard VAR-001-2 — Voltage and Reactive Control

- R6.** The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.
- R6.1.** When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.
- R7.** The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.
- R8.** Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.
- R9.** Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; and controllable load– to support its voltage under first Contingency conditions.
- R9.1.** Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.
- R10.** Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.
- R11.** After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.
- R12.** The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

C. Measures

- M1.** The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule as specified in Requirement 4 to each Generator Operator it requires to follow such a schedule.
- M2.** The Transmission Operator shall have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3.2.
- M3.** The Transmission Operator shall have evidence to show that it issued directives as specified in Requirement 6.1 when notified by a Generator Operator of the loss of an automatic voltage regulator control.
- M4.** The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with Requirement 11.

D. Compliance

- 1. Compliance Monitoring Process**

Standard VAR-001-2 — Voltage and Reactive Control

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months.

The Compliance Monitor shall retain any audit data for three years.

1.5. Additional Compliance Information

The Transmission Operator 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.

2. Violation Severity Levels (no changes)

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	TBD	Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised.
2	August 5, 2010	Adopted by the NERC Board of Trustees	
2	January 10, 2011	Approved by FERC	
2	February 7, 2013	R5 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending	

Standard VAR-001-2 — Voltage and Reactive Control

		applicable regulatory approval.	
2	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard VAR-001-2 — Voltage and Reactive Control

United States

Standard	Requirement	Enforcement Date	Inactive Date
VAR-001-2	R1.	10/01/2011	12/31/2013
VAR-001-2	R2.	10/01/2011	12/31/2013
VAR-001-2	R3.	10/01/2011	12/31/2013
VAR-001-2	R3.1.	10/01/2011	12/31/2013
VAR-001-2	R3.2.	10/01/2011	12/31/2013
VAR-001-2	R4.	10/01/2011	12/31/2013
VAR-001-2	R5.	10/01/2011	01/21/2014
VAR-001-2	R6.	10/01/2011	12/31/2013
VAR-001-2	R6.1.	10/01/2011	12/31/2013
VAR-001-2	R7.	10/01/2011	12/31/2013
VAR-001-2	R8.	10/01/2011	12/31/2013
VAR-001-2	R9.	10/01/2011	12/31/2013
VAR-001-2	R9.1.	10/01/2011	12/31/2013
VAR-001-2	R10.	10/01/2011	12/31/2013
VAR-001-2	R11.	10/01/2011	12/31/2013
VAR-001-2	R12.	10/01/2011	12/31/2013

Exhibit A(3): Updated NERC Glossary of Terms for Approval

Glossary of Terms Used in NERC Reliability Standards

Updated February 13, 2014

Introduction:

This Glossary lists each term that was defined for use in one or more of NERC's continent-wide or Regional Reliability Standards and adopted by the NERC Board of Trustees from February 8, 2005 through February 13, 2014.

This reference is divided into two sections, and each section is organized in alphabetical order. The first section identifies all terms that have been adopted by the NERC Board of Trustees for use in continent-wide standards; the second section identifies all terms that have been adopted by the NERC Board of Trustees for use in regional standards. (WECC, NPCC and *ReliabilityFirst* are the only Regions that have definitions approved by the NERC Board of Trustees. If other Regions develop definitions for approved Regional Standards using a NERC-approved standards development process, those definitions will be added to the Regional Definitions section of this glossary.)

Most of the terms identified in this glossary were adopted as part of the development of NERC's initial set of reliability standards, called the "Version 0" standards. Subsequent to the development of Version 0 standards, new definitions have been developed and approved following NERC's Reliability Standards Development Process, and added to this glossary following board adoption, with the "FERC approved" date added following a final Order approving the definition.

Immediately under each term is a link to the archive for the development of that term.

Definitions that have been adopted by the NERC Board of Trustees but have not been approved by FERC, or FERC has not approved but has directed be modified, are shaded in blue. Definitions that have been remanded or retired are shaded in orange.

Any comments regarding this glossary should be reported to the following:
sarcomm@nerc.com with "Glossary Comment" in the subject line.

Continent-wide Definitions:

A..... 5

B..... 9

C..... 22

D..... 27

E..... 30

F..... 33

G..... 37

H..... 38

I..... 39

J..... 43

L..... 44

M..... 44

N..... 46

O..... 49

P..... 53

R..... 59

S..... 71

T..... 74

V..... 78

W..... 79

Y 79

Regional Definitions:

ERCOT Regional Definitions 80

NPCC Regional Definitions 82

Reliability*First* Regional Definitions 83

WECC Regional Definitions 84

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Adequacy [Archive]		2/8/2005	3/16/2007	The ability of the electric system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.
Adjacent Balancing Authority [Archive]		2/8/2005	3/16/2007	A Balancing Authority Area that is interconnected another Balancing Authority Area either directly or via a multi-party agreement or transmission tariff.
Adverse Reliability Impact [Archive]		2/7/2006	3/16/2007	The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection.
Adverse Reliability Impact [Archive]		8/4/2011		The impact of an event that results in Bulk Electric System instability or Cascading.
After the Fact [Archive]	ATF	10/29/2008	12/17/2009	A time classification assigned to an RFI when the submittal time is greater than one hour after the start time of the RFI.
Agreement [Archive]		2/8/2005	3/16/2007	A contract or arrangement, either written or verbal and sometimes enforceable by law.
Alternative Interpersonal Communication [Archive]		11/7/2012		Any Interpersonal Communication that is able to serve as a substitute for, and does not utilize the same infrastructure (medium) as, Interpersonal Communication used for day-to-day operation.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Altitude Correction Factor [Archive]		2/7/2006	3/16/2007	A multiplier applied to specify distances, which adjusts the distances to account for the change in relative air density (RAD) due to altitude from the RAD used to determine the specified distance. Altitude correction factors apply to both minimum worker approach distances and to minimum vegetation clearance distances.
Ancillary Service [Archive]		2/8/2005	3/16/2007	Those services that are necessary to support the transmission of capacity and energy from resources to loads while maintaining reliable operation of the Transmission Service Provider's transmission system in accordance with good utility practice. <i>(From FERC order 888-A.)</i>
Anti-Aliasing Filter [Archive]		2/8/2005	3/16/2007	An analog filter installed at a metering point to remove the high frequency components of the signal over the AGC sample period.
Area Control Error [Archive]	ACE	2/8/2005	3/16/2007 (Becomes inactive 3/31/14)	The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias and correction for meter error.
Area Control Error [Archive]	ACE	12/19/2012	10/16/2013 (Becomes effective 4/1/2014)	The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias, correction for meter error, and Automatic Time Error Correction (ATEC), if operating in the ATEC mode. ATEC is only applicable to Balancing Authorities in the Western Interconnection.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Area Interchange Methodology [Archive]		08/22/2008	11/24/2009	The Area Interchange methodology is characterized by determination of incremental transfer capability via simulation, from which Total Transfer Capability (TTC) can be mathematically derived. Capacity Benefit Margin, Transmission Reliability Margin, and Existing Transmission Commitments are subtracted from the TTC, and Postbacks and counterflows are added, to derive Available Transfer Capability. Under the Area Interchange Methodology, TTC results are generally reported on an area to area basis.
Arranged Interchange [Archive]		5/2/2006	3/16/2007	The state where the Interchange Authority has received the Interchange information (initial or revised).
Automatic Generation Control [Archive]	AGC	2/8/2005	3/16/2007	Equipment that automatically adjusts generation in a Balancing Authority Area from a central location to maintain the Balancing Authority's interchange schedule plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction.
Available Flowgate Capability [Archive]	AFC	08/22/2008	11/24/2009	A measure of the flow capability remaining on a Flowgate for further commercial activity over and above already committed uses. It is defined as TFC less Existing Transmission Commitments (ETC), less a Capacity Benefit Margin, less a Transmission Reliability Margin, plus Postbacks, and plus counterflows.
Available Transfer Capability [Archive]	ATC	2/8/2005	3/16/2007	A measure of the transfer capability remaining in the physical transmission network for further commercial activity over and above already committed uses. It is defined as Total Transfer Capability less existing transmission commitments (including retail customer service), less a Capacity Benefit Margin, less a Transmission Reliability Margin.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Available Transfer Capability [Archive]	ATC	08/22/2008	11/24/2009	A measure of the transfer capability remaining in the physical transmission network for further commercial activity over and above already committed uses. It is defined as Total Transfer Capability less Existing Transmission Commitments (including retail customer service), less a Capacity Benefit Margin, less a Transmission Reliability Margin, plus Postbacks, plus counterflows.
Available Transfer Capability Implementation Document [Archive]	ATCID	08/22/2008	11/24/2009	A document that describes the implementation of a methodology for calculating ATC or AFC, and provides information related to a Transmission Service Provider's calculation of ATC or AFC.
ATC Path [Archive]		08/22/2008	Not approved; Modification directed 11/24/09	Any combination of Point of Receipt and Point of Delivery for which ATC is calculated; and any Posted Path ¹ .

¹ See 18 CFR 37.6(b)(1)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Balancing Authority [Archive]	BA	2/8/2005	3/16/2007	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
Balancing Authority Area [Archive]		2/8/2005	3/16/2007	The collection of generation, transmission, and loads within the metered boundaries of the Balancing Authority. The Balancing Authority maintains load-resource balance within this area.
Base Load [Archive]		2/8/2005	3/16/2007	The minimum amount of electric power delivered or required over a given period at a constant rate.
BES Cyber Asset [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
BES Cyber System [Archive]		11/26/12	11/22/13 (Becomes effective 4/1/16)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
BES Cyber System Information [Archive]		11/26/12	11/22/13 (Becomes effective 4/1/16)	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Blackstart Capability Plan [Archive]		2/8/2005 Will be retired when EOP-005-2 becomes enforceable on (7/1/13)	3/16/2007	A documented procedure for a generating unit or station to go from a shutdown condition to an operating condition delivering electric power without assistance from the electric system. This procedure is only a portion of an overall system restoration plan.
Blackstart Resource [Archive]		8/5/2009	3/17/11	A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan.
Block Dispatch [Archive]		08/22/2008	11/24/2009	A set of dispatch rules such that given a specific amount of load to serve, an approximate generation dispatch can be determined. To accomplish this, the capacity of a given generator is segmented into loadable "blocks," each of which is grouped and ordered relative to other blocks (based on characteristics including, but not limited to, efficiency, run of river or fuel supply considerations, and/or "must-run" status).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System [Archive]	BES	2/8/2005	3/16/2007 (Becomes inactive on 6/30/14)	As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System ² [Archive]	BES	01/18/2012	6/14/13 (Becomes effective 7/1/14)	Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. Inclusions: <ul style="list-style-type: none"> • I1 - Transformers with the primary terminal and at least one secondary terminal operated at 100 kV or higher unless excluded under Exclusion E1 or E3. • I2 - Generating resource(s) with gross individual nameplate rating greater than 20 MVA or gross plant/facility aggregate nameplate rating greater than 75 MVA including the generator terminals through the high-side of the step-up transformer(s) connected at a voltage of 100 kV or above. • I3 - Blackstart Resources identified in the Transmission Operator's restoration plan. • I4 - Dispersed power producing resources with aggregate capacity greater than 75 MVA (gross aggregate nameplate rating) utilizing a system designed primarily for aggregating capacity, connected at a common point at a voltage of 100 kV or above.

² FERC issued an order on April 18, 2013 approving the revised definition with an effective date of July 1, 2013. On June 14, 2013, FERC granted NERC's request to extend the effective date of the revised definition of the Bulk Electric System to July 1, 2014.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System (Continued)	BES			<p>I5 –Static or dynamic devices (excluding generators) dedicated to supplying or absorbing Reactive Power that are connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, or through a transformer that is designated in Inclusion I1.</p> <p>Exclusions:</p> <ul style="list-style-type: none"> • E1 - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: <ul style="list-style-type: none"> a) Only serves Load. Or, b) Only includes generation resources, not identified in Inclusion I3, with an aggregate capacity less than or equal to 75 MVA (gross nameplate rating). Or, c) Where the radial system serves Load and includes generation resources, not identified in Inclusion I3, with an aggregate capacity of non-retail generation less than or equal to 75 MVA (gross nameplate rating). <p>Note – A normally open switching device between radial systems, as depicted on prints or one-line diagrams for example, does not affect this exclusion.</p>

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System (Continued)	BES			<ul style="list-style-type: none"> • E2 - A generating unit or multiple generating units on the customer’s side of the retail meter that serve all or part of the retail Load with electric energy if: (i) the net capacity provided to the BES does not exceed 75 MVA, and (ii) standby, back-up, and maintenance power services are provided to the generating unit or multiple generating units or to the retail Load by a Balancing Authority, or provided pursuant to a binding obligation with a Generator Owner or Generator Operator, or under terms approved by the applicable regulatory authority. • E3 - Local networks (LN): A group of contiguous transmission Elements operated at or above 100 kV but less than 300 kV that distribute power to Load rather than transfer bulk power across the interconnected system. LN’s emanate from multiple points of connection at 100 kV or higher to improve the level of service to retail customer Load and not to accommodate bulk power transfer across the interconnected system. The LN is characterized by all of the following:

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System (Continued)	BES			<ul style="list-style-type: none"> a) Limits on connected generation: The LN and its underlying Elements do not include generation resources identified in Inclusion I3 and do not have an aggregate capacity of non-retail generation greater than 75 MVA (gross nameplate rating); b) Power flows only into the LN and the LN does not transfer energy originating outside the LN for delivery through the LN; and c) Not part of a Flowgate or transfer path: The LN does not contain a monitored Facility of a permanent Flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection, or a comparable monitored Facility in the ERCOT or Quebec Interconnections, and is not a monitored Facility included in an Interconnection Reliability Operating Limit (IROL). <ul style="list-style-type: none"> • E4 – Reactive Power devices owned and operated by the retail customer solely for its own use. Note - Elements may be included or excluded on a case-by-case basis through the Rules of Procedure exception process.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System [Archive]	BES	11/21/2013		<p>Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.</p> <p>Inclusions:</p> <ul style="list-style-type: none"> • I1 - Transformers with the primary terminal and at least one secondary terminal operated at 100 kV or higher unless excluded by application of Exclusion E1 or E3. • I2 – Generating resource(s) including the generator terminals through the high-side of the step-up transformer(s) connected at a voltage of 100 kV or above with: <ul style="list-style-type: none"> a) Gross individual nameplate rating greater than 20 MVA. Or, b) Gross plant/facility aggregate nameplate rating greater than 75 MVA. • I3 - Blackstart Resources identified in the Transmission Operator’s restoration plan. • I4 - Dispersed power producing resources that aggregate to a total capacity greater than 75 MVA (gross nameplate rating), and that are connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage of 100 kV or above. <p>Thus, the facilities designated as BES are:</p>

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System (Continued)	BES			<ul style="list-style-type: none"> a) The individual resources, and b) The system designed primarily for delivering capacity from the point where those resources aggregate to greater than 75 MVA to a common point of connection at a voltage of 100 kV or above. <ul style="list-style-type: none"> • I5 –Static or dynamic devices (excluding generators) dedicated to supplying or absorbing Reactive Power that are connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, or through a transformer that is designated in Inclusion I1 unless excluded by application of Exclusion E4. <p>Exclusions:</p> <ul style="list-style-type: none"> • E1 - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: <ul style="list-style-type: none"> a) Only serves Load. Or, b) Only includes generation resources, not identified in Inclusions I2, I3, or I4, with an aggregate capacity less than or equal to 75 MVA (gross nameplate rating). Or, c) Where the radial system serves Load and includes generation resources, not identified in Inclusions I2, I3 or I4, with an aggregate capacity of non-retail generation less than or equal to 75 MVA (gross nameplate rating).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System (Continued)	BES			<p>Note 1 – A normally open switching device between radial systems, as depicted on prints or one-line diagrams for example, does not affect this exclusion.</p> <p>Note 2 – The presence of a contiguous loop, operated at a voltage level of 50 kV or less, between configurations being considered as radial systems, does not affect this exclusion.</p> <ul style="list-style-type: none"> • E2 - A generating unit or multiple generating units on the customer’s side of the retail meter that serve all or part of the retail Load with electric energy if: (i) the net capacity provided to the BES does not exceed 75 MVA, and (ii) standby, back-up, and maintenance power services are provided to the generating unit or multiple generating units or to the retail Load by a Balancing Authority, or provided pursuant to a binding obligation with a Generator Owner or Generator Operator, or under terms approved by the applicable regulatory authority. • E3 - Local networks (LN): A group of contiguous transmission Elements operated at less than 300 kV that distribute power to Load rather than transfer bulk power across the interconnected system. LN’s emanate from multiple points of connection at 100 kV or higher to improve the level of service to retail customers and not to accommodate bulk power transfer across the interconnected system. The LN is characterized by all of the following: <ul style="list-style-type: none"> a) Limits on connected generation: The LN and its underlying Elements do not include generation resources identified in Inclusions I2, I3, or I4 and do not have an aggregate capacity of non-retail

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System (Continued)	BES			<p>generation greater than 75 MVA (gross nameplate rating);</p> <p>b) Real Power flows only into the LN and the LN does not transfer energy originating outside the LN for delivery through the LN; and</p> <p>c) Not part of a Flowgate or transfer path: The LN does not contain any part of a permanent Flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection, or a comparable monitored Facility in the ERCOT or Quebec Interconnections, and is not a monitored Facility included in an Interconnection Reliability Operating Limit (IROL).</p> <ul style="list-style-type: none"> • E4 – Reactive Power devices installed for the sole benefit of a retail customer(s). <p>Note - Elements may be included or excluded on a case-by-case basis through the Rules of Procedure exception process.</p>
Bulk-Power System [Archive]		5/9/2013	7/9/2013	<p>A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.</p>

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Burden [Archive]		2/8/2005	3/16/2007	Operation of the Bulk Electric System that violates or is expected to violate a System Operating Limit or Interconnection Reliability Operating Limit in the Interconnection, or that violates any other NERC, Regional Reliability Organization, or local operating reliability standards or criteria.
Business Practices [Archive]		8/22/2008	Not approved; Modification directed 11/24/09	Those business rules contained in the Transmission Service Provider’s applicable tariff, rules, or procedures; associated Regional Reliability Organization or regional entity business practices; or NAESB Business Practices.
Bus-tie Breaker [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/15)	A circuit breaker that is positioned to connect two individual substation bus configurations.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Capacity Benefit Margin [Archive]	CBM	2/8/2005	3/16/2007	The amount of firm transmission transfer capability preserved by the transmission provider for Load-Serving Entities (LSEs), whose loads are located on that Transmission Service Provider's system, to enable access by the LSEs to generation from interconnected systems to meet generation reliability requirements. Preservation of CBM for an LSE allows that entity to reduce its installed generating capacity below that which may otherwise have been necessary without interconnections to meet its generation reliability requirements. The transmission transfer capability preserved as CBM is intended to be used by the LSE only in times of emergency generation deficiencies.
Capacity Benefit Margin Implementation Document [Archive]	CBMID	11/13/2008	11/24/2009	A document that describes the implementation of a Capacity Benefit Margin methodology.
Capacity Emergency [Archive]		2/8/2005	3/16/2007	A capacity emergency exists when a Balancing Authority Area's operating capacity, plus firm purchases from other systems, to the extent available or limited by transfer capability, is inadequate to meet its demand plus its regulating requirements.
Cascading [Archive]		2/8/2005	3/16/2007	The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Cascading Outages [Archive]		11/1/2006 Withdrawn 2/12/2008	FERC Remanded 12/27/2007	The uncontrolled successive loss of Bulk Electric System Facilities triggered by an incident (or condition) at any location resulting in the interruption of electric service that cannot be restrained from spreading beyond a pre-determined area.
CIP Exceptional Circumstance [Archive]		11/26/12	11/22/13 (Becomes effective 4/1/16)	A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.
CIP Senior Manager [Archive]		11/26/12	11/22/13 (Becomes effective 4/1/16)	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.
Clock Hour [Archive]		2/8/2005	3/16/2007	The 60-minute period ending at :00. All surveys, measurements, and reports are based on Clock Hour periods unless specifically noted.
Cogeneration [Archive]		2/8/2005	3/16/2007	Production of electricity from steam, heat, or other forms of energy produced as a by-product of another process.
Compliance Monitor [Archive]		2/8/2005	3/16/2007	The entity that monitors, reviews, and ensures compliance of responsible entities with reliability standards.
Confirmed Interchange [Archive]		5/2/2006	3/16/2007	The state where the Interchange Authority has verified the Arranged Interchange.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Congestion Management Report [Archive]		2/8/2005	3/16/2007	A report that the Interchange Distribution Calculator issues when a Reliability Coordinator initiates the Transmission Loading Relief procedure. This report identifies the transactions and native and network load curtailments that must be initiated to achieve the loading relief requested by the initiating Reliability Coordinator.
Consequential Load Loss [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/15)	All Load that is no longer served by the Transmission system as a result of Transmission Facilities being removed from service by a Protection System operation designed to isolate the fault.
Constrained Facility [Archive]		2/8/2005	3/16/2007	A transmission facility (line, transformer, breaker, etc.) that is approaching, is at, or is beyond its System Operating Limit or Interconnection Reliability Operating Limit.
Contingency [Archive]		2/8/2005	3/16/2007	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element.
Contingency Reserve [Archive]		2/8/2005	3/16/2007	The provision of capacity deployed by the Balancing Authority to meet the Disturbance Control Standard (DCS) and other NERC and Regional Reliability Organization contingency requirements.
Contract Path [Archive]		2/8/2005	3/16/2007	An agreed upon electrical path for the continuous flow of electrical power between the parties of an Interchange Transaction.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Control Center [Archive]		11/26/12	11/22/13 (Becomes effective 4/1/16)	One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
Control Performance Standard [Archive]	CPS	2/8/2005	3/16/2007	The reliability standard that sets the limits of a Balancing Authority's Area Control Error over a specified time period.
Corrective Action Plan [Archive]		2/7/2006	3/16/2007	A list of actions and an associated timetable for implementation to remedy a specific problem.
Cranking Path [Archive]		5/2/2006	3/16/2007	A portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units.
Critical Assets [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/16)	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
Critical Cyber Assets [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/16)	Cyber Assets essential to the reliable operation of Critical Assets.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Curtailment [Archive]		2/8/2005	3/16/2007	A reduction in the scheduled capacity or energy delivery of an Interchange Transaction.
Curtailment Threshold [Archive]		2/8/2005	3/16/2007	The minimum Transfer Distribution Factor which, if exceeded, will subject an Interchange Transaction to curtailment to relieve a transmission facility constraint.
Cyber Assets [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/16)	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber Assets [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	Programmable electronic devices, including the hardware, software, and data in those devices.
Cyber Security Incident [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/16)	Any malicious act or suspicious event that: <ul style="list-style-type: none"> • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.
Cyber Security Incident [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	A malicious act or suspicious event that: <ul style="list-style-type: none"> • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Delayed Fault Clearing [Archive]		11/1/2006	12/27/2007	Fault clearing consistent with correct operation of a breaker failure protection system and its associated breakers, or of a backup protection system with an intentional time delay.
Demand [Archive]		2/8/2005	3/16/2007	<ol style="list-style-type: none"> 1. The rate at which electric energy is delivered to or by a system or part of a system, generally expressed in kilowatts or megawatts, at a given instant or averaged over any designated interval of time. 2. The rate at which energy is being used by the customer.
Demand-Side Management [Archive]	DSM	2/8/2005	3/16/2007	The term for all activities or programs undertaken by Load-Serving Entity or its customers to influence the amount or timing of electricity they use.
Dial-up Connectivity [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.
Direct Control Load Management [Archive]	DCLM	2/8/2005	3/16/2007	Demand-Side Management that is under the direct control of the system operator. DCLM may control the electric supply to individual appliances or equipment on customer premises. DCLM as defined here does not include Interruptible Demand.
Dispatch Order [Archive]		08/22/2008	11/24/2009	A set of dispatch rules such that given a specific amount of load to serve, an approximate generation dispatch can be determined. To accomplish this, each generator is ranked by priority.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Dispersed Load by Substations [Archive]		2/8/2005	3/16/2007	Substation load information configured to represent a system for power flow or system dynamics modeling purposes, or both.
Distribution Factor [Archive]	DF	2/8/2005	3/16/2007	The portion of an Interchange Transaction, typically expressed in per unit that flows across a transmission facility (Flowgate).
Distribution Provider [Archive]	DP	2/8/2005	3/16/2007	Provides and operates the “wires” between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the Transmission Owner also serves as the Distribution Provider. Thus, the Distribution Provider is not defined by a specific voltage, but rather as performing the Distribution function at any voltage.
Disturbance [Archive]		2/8/2005	3/16/2007	<ol style="list-style-type: none"> 1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.
Disturbance Control Standard [Archive]	DCS	2/8/2005	3/16/2007	The reliability standard that sets the time limit following a Disturbance within which a Balancing Authority must return its Area Control Error to within a specified range.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Disturbance Monitoring Equipment [Archive]	DME	8/2/2006	3/16/2007	<p>Devices capable of monitoring and recording system data pertaining to a Disturbance. Such devices include the following categories of recorders³:</p> <ul style="list-style-type: none"> • Sequence of event recorders which record equipment response to the event • Fault recorders, which record actual waveform data replicating the system primary voltages and currents. This may include protective relays. • Dynamic Disturbance Recorders (DDRs), which record incidents that portray power system behavior during dynamic events such as low-frequency (0.1 Hz – 3 Hz) oscillations and abnormal frequency or voltage excursions
Dynamic Interchange Schedule or Dynamic Schedule [Archive]		2/8/2005	3/16/2007	A telemetered reading or value that is updated in real time and used as a schedule in the AGC/ACE equation and the integrated value of which is treated as a schedule for interchange accounting purposes. Commonly used for scheduling jointly owned generation to or from another Balancing Authority Area.
Dynamic Transfer [Archive]		2/8/2005	3/16/2007	The provision of the real-time monitoring, telemetering, computer software, hardware, communications, engineering, energy accounting (including inadvertent interchange), and administration required to electronically move all or a portion of the real energy services associated with a generator or load out of one Balancing Authority Area into another.

³ Phasor Measurement Units and any other equipment that meets the functional requirements of DMEs may qualify as DMEs.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Economic Dispatch [Archive]		2/8/2005	3/16/2007	The allocation of demand to individual generating units on line to effect the most economical production of electricity.
Electronic Access Control or Monitoring Systems [Archive]	EACMS	11/26/12	11/22/2013 (Becomes effective 4/1/16)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.
Electronic Access Point [Archive]	EAP	11/26/12	11/22/2013 (Becomes effective 4/1/16)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
Electrical Energy [Archive]		2/8/2005	3/16/2007	The generation or use of electric power by a device over a period of time, expressed in kilowatthours (kWh), megawatthours (MWh), or gigawatthours (GWh).
Electronic Security Perimeter [Archive]	ESP	5/2/2006	1/18/2008 (Becomes inactive 3/31/16)	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
Electronic Security Perimeter [Archive]	ESP	11/26/12	11/22/2013 (Becomes effective 4/1/16)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Element [Archive]		2/8/2005	3/16/2007	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components.
Emergency or BES Emergency [Archive]		2/8/2005	3/16/2007	Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System.
Emergency Rating [Archive]		2/8/2005	3/16/2007	The rating as defined by the equipment owner that specifies the level of electrical loading or output, usually expressed in megawatts (MW) or Mvar or other appropriate units, that a system, facility, or element can support, produce, or withstand for a finite period. The rating assumes acceptable loss of equipment life or other physical or safety limitations for the equipment involved.
Emergency Request for Interchange [Archive]	Emergency RFI	10/29/2008	12/17/2009	Request for Interchange to be initiated for Emergency or Energy Emergency conditions.
Energy Emergency [Archive]		2/8/2005	3/16/2007	A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers' expected energy requirements.
Equipment Rating [Archive]		2/7/2006	3/16/2007	The maximum and minimum voltage, current, frequency, real and reactive power flows on individual equipment under steady state, short-circuit and transient conditions, as permitted or assigned by the equipment owner.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
External Routable Connectivity [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
Existing Transmission Commitments [Archive]	ETC	08/22/2008	11/24/2009	Committed uses of a Transmission Service Provider's Transmission system considered when determining ATC or AFC.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Facility [Archive]		2/7/2006	3/16/2007	A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)
Facility Rating [Archive]		2/8/2005	3/16/2007	The maximum or minimum voltage, current, frequency, or real or reactive power flow through a facility that does not violate the applicable equipment rating of any equipment comprising the facility.
Fault [Archive]		2/8/2005	3/16/2007	An event occurring on an electric system such as a short circuit, a broken wire, or an intermittent connection.
Fire Risk [Archive]		2/7/2006	3/16/2007	The likelihood that a fire will ignite or spread in a particular geographic area.
Firm Demand [Archive]		2/8/2005	3/16/2007	That portion of the Demand that a power supplier is obligated to provide except when system reliability is threatened or during emergency conditions.
Firm Transmission Service [Archive]		2/8/2005	3/16/2007	The highest quality (priority) service offered to customers under a filed rate schedule that anticipates no planned interruption.
Flashover [Archive]		2/7/2006	3/16/2007	An electrical discharge through air around or over the surface of insulation, between objects of different potential, caused by placing a voltage across the air space that results in the ionization of the air space.
Flowgate [Archive]		2/8/2005	3/16/2007	A designated point on the transmission system through which the Interchange Distribution Calculator calculates the power flow from Interchange Transactions.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Flowgate [Archive]		08/22/2008	11/24/2009	<p>1.) A portion of the Transmission system through which the Interchange Distribution Calculator calculates the power flow from Interchange Transactions.</p> <p>2.) A mathematical construct, comprised of one or more monitored transmission Facilities and optionally one or more contingency Facilities, used to analyze the impact of power flows upon the Bulk Electric System.</p>
Flowgate Methodology [Archive]		08/22/2008	11/24/2009	The Flowgate methodology is characterized by identification of key Facilities as Flowgates. Total Flowgate Capabilities are determined based on Facility Ratings and voltage and stability limits. The impacts of Existing Transmission Commitments (ETCs) are determined by simulation. The impacts of ETC, Capacity Benefit Margin (CBM) and Transmission Reliability Margin (TRM) are subtracted from the Total Flowgate Capability, and Postbacks and counterflows are added, to determine the Available Flowgate Capability (AFC) value for that Flowgate. AFCs can be used to determine Available Transfer Capability (ATC).
Forced Outage [Archive]		2/8/2005	3/16/2007	<p>1. The removal from service availability of a generating unit, transmission line, or other facility for emergency reasons.</p> <p>2. The condition in which the equipment is unavailable due to unanticipated failure.</p>
Frequency Bias [Archive]		2/8/2005	3/16/2007	A value, usually expressed in megawatts per 0.1 Hertz (MW/0.1 Hz), associated with a Balancing Authority Area that approximates the Balancing Authority Area's response to Interconnection frequency error.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Bias Setting [Archive]		2/8/2005	3/16/2007 (Becomes inactive 3/31/15)	A value, usually expressed in MW/0.1 Hz, set into a Balancing Authority ACE algorithm that allows the Balancing Authority to contribute its frequency response to the Interconnection.
Frequency Bias Setting [Archive]		2/7/2013	1/16/2014 (Becomes effective 4/1/15)	A number, either fixed or variable, usually expressed in MW/0.1 Hz, included in a Balancing Authority's Area Control Error equation to account for the Balancing Authority's inverse Frequency Response contribution to the Interconnection, and discourage response withdrawal through secondary control systems.
Frequency Deviation [Archive]		2/8/2005	3/16/2007	A change in Interconnection frequency.
Frequency Error [Archive]		2/8/2005	3/16/2007	The difference between the actual and scheduled frequency. (F _A – F _S)
Frequency Regulation [Archive]		2/8/2005	3/16/2007	The ability of a Balancing Authority to help the Interconnection maintain Scheduled Frequency. This assistance can include both turbine governor response and Automatic Generation Control.
Frequency Response [Archive]		2/8/2005	3/16/2007	(Equipment) The ability of a system or elements of the system to react or respond to a change in system frequency. (System) The sum of the change in demand, plus the change in generation, divided by the change in frequency, expressed in megawatts per 0.1 Hertz (MW/0.1 Hz).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Response Measure [Archive]	FRM	2/7/2013	1/16/2014 (Becomes effective 4/1/15)	The median of all the Frequency Response observations reported annually by Balancing Authorities or Frequency Response Sharing Groups for frequency events specified by the ERO. This will be calculated as MW/0.1Hz.
Frequency Response Obligation [Archive]	FRO	2/7/2013	1/16/2014 (Becomes effective 4/1/15)	The Balancing Authority's share of the required Frequency Response needed for the reliable operation of an Interconnection. This will be calculated as MW/0.1Hz.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Response Sharing Group [Archive]	FRSG	2/7/2013	1/16/2014 (Becomes effective 4/1/15)	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply operating resources required to jointly meet the sum of the Frequency Response Obligations of its members.
Generator Operator [Archive]	GOP	2/8/2005	3/16/2007	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
Generator Owner [Archive]	GO	2/8/2005	3/16/2007	Entity that owns and maintains generating units.
Generator Shift Factor [Archive]	GSF	2/8/2005	3/16/2007	A factor to be applied to a generator's expected change in output to determine the amount of flow contribution that change in output will impose on an identified transmission facility or Flowgate.
Generator-to-Load Distribution Factor [Archive]	GLDF	2/8/2005	3/16/2007	The algebraic sum of a Generator Shift Factor and a Load Shift Factor to determine the total impact of an Interchange Transaction on an identified transmission facility or Flowgate.
Generation Capability Import Requirement [Archive]	GCIR	11/13/2008	11/24/2009	The amount of generation capability from external sources identified by a Load-Serving Entity (LSE) or Resource Planner (RP) to meet its generation reliability or resource adequacy requirements as an alternative to internal resources.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Host Balancing Authority [Archive]		2/8/2005	3/16/2007	<ol style="list-style-type: none"> 1. A Balancing Authority that confirms and implements Interchange Transactions for a Purchasing Selling Entity that operates generation or serves customers directly within the Balancing Authority's metered boundaries. 2. The Balancing Authority within whose metered boundaries a jointly owned unit is physically located.
Hourly Value [Archive]		2/8/2005	3/16/2007	Data measured on a Clock Hour basis.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Implemented Interchange [Archive]		5/2/2006	3/16/2007	The state where the Balancing Authority enters the Confirmed Interchange into its Area Control Error equation.
Inadvertent Interchange [Archive]		2/8/2005	3/16/2007	The difference between the Balancing Authority's Net Actual Interchange and Net Scheduled Interchange. (I _A – I _S)
Independent Power Producer [Archive]	IPP	2/8/2005	3/16/2007	Any entity that owns or operates an electricity generating facility that is not included in an electric utility's rate base. This term includes, but is not limited to, cogenerators and small power producers and all other nonutility electricity producers, such as exempt wholesale generators, who sell electricity.
Institute of Electrical and Electronics Engineers, Inc. [Archive]	IEEE	2/7/2006	3/16/2007	

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interactive Remote Access [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
Interchange [Archive]		5/2/2006	3/16/2007	Energy transfers that cross Balancing Authority boundaries.
Interchange Authority [Archive]	IA	5/2/2006	3/16/2007	The responsible entity that authorizes implementation of valid and balanced Interchange Schedules between Balancing Authority Areas, and ensures communication of Interchange information for reliability assessment purposes.
Interchange Distribution Calculator [Archive]	IDC	2/8/2005	3/16/2007	The mechanism used by Reliability Coordinators in the Eastern Interconnection to calculate the distribution of Interchange Transactions over specific Flowgates. It includes a database of all Interchange Transactions and a matrix of the Distribution Factors for the Eastern Interconnection.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interchange Schedule [Archive]		2/8/2005	3/16/2007	An agreed-upon Interchange Transaction size (megawatts), start and end time, beginning and ending ramp times and rate, and type required for delivery and receipt of power and energy between the Source and Sink Balancing Authorities involved in the transaction.
Interchange Transaction [Archive]		2/8/2005	3/16/2007	An agreement to transfer energy from a seller to a buyer that crosses one or more Balancing Authority Area boundaries.
Interchange Transaction Tag or Tag [Archive]		2/8/2005	3/16/2007	The details of an Interchange Transaction required for its physical implementation.
Interconnected Operations Service [Archive]		2/8/2005	3/16/2007	A service (exclusive of basic energy and transmission services) that is required to support the reliable operation of interconnected Bulk Electric Systems.
Interconnection [Archive]		2/8/2005	3/16/2007	When capitalized, any one of the three major electric system networks in North America: Eastern, Western, and ERCOT.
Interconnection [Archive]		8/15/2013		When capitalized, any one of the four major electric system networks in North America: Eastern, Western, ERCOT and Quebec.
Interconnection Reliability Operating Limit [Archive]	IROL	2/8/2005	3/16/2007 Retired 12/27/2007	The value (such as MW, MVar, Amperes, Frequency or Volts) derived from, or a subset of the System Operating Limits, which if exceeded, could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interconnection Reliability Operating Limit [Archive]	IROL	11/1/2006	12/27/2007	A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages ⁴ that adversely impact the reliability of the Bulk Electric System.
Interconnection Reliability Operating Limit T _v [Archive]	IROL T _v	11/1/2006	12/27/2007	The maximum time that an Interconnection Reliability Operating Limit can be violated before the risk to the interconnection or other Reliability Coordinator Area(s) becomes greater than acceptable. Each Interconnection Reliability Operating Limit's T _v shall be less than or equal to 30 minutes.
Intermediate Balancing Authority [Archive]		2/8/2005	3/16/2007	A Balancing Authority Area that has connecting facilities in the Scheduling Path between the Sending Balancing Authority Area and Receiving Balancing Authority Area and operating agreements that establish the conditions for the use of such facilities.
Intermediate System [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.
Interpersonal Communication [Archive]		11/7/2012		Any medium that allows two or more individuals to interact, consult, or exchange information.

⁴ On September 13, 2012, FERC issued an Order approving NERC's request to modify the reference to "Cascading Outages" to "Cascading outages" within the definition of IROL due to the fact that the definition of "Cascading Outages" was previously remanded by FERC.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interruptible Load or Interruptible Demand [Archive]		11/1/2006	3/16/2007	Demand that the end-use customer makes available to its Load-Serving Entity via contract or agreement for curtailment.
Joint Control [Archive]		2/8/2005	3/16/2007	Automatic Generation Control of jointly owned units by two or more Balancing Authorities.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Limiting Element [Archive]		2/8/2005	3/16/2007	The element that is 1.)Either operating at its appropriate rating, or 2,) Would be following the limiting contingency. Thus, the Limiting Element establishes a system limit.
Load [Archive]		2/8/2005	3/16/2007	An end-use device or customer that receives power from the electric system.
Load Shift Factor [Archive]	LSF	2/8/2005	3/16/2007	A factor to be applied to a load’s expected change in demand to determine the amount of flow contribution that change in demand will impose on an identified transmission facility or monitored Flowgate.
Load-Serving Entity [Archive]	LSE	2/8/2005	3/16/2007	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.
Long-Term Transmission Planning Horizon [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/15)	Transmission planning period that covers years six through ten or beyond when required to accommodate any known longer lead time projects that may take longer than ten years to complete.
Market Flow [Archive]		11/4/2010	4/21/2011	The total amount of power flowing across a specified Facility or set of Facilities due to a market dispatch of generation internal to the market to serve load internal to the market.
Minimum Vegetation Clearance Distance [Archive]	MVCD	11/3/2011	3/21/2013 (Becomes effective 7/1/14)	The calculated minimum distance stated in feet (meters) to prevent flash-over between conductors and vegetation, for various altitudes and operating voltages.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Misoperation [Archive]		2/7/2006	3/16/2007	<ul style="list-style-type: none"> Any failure of a Protection System element to operate within the specified time when a fault or abnormal condition occurs within a zone of protection. Any operation for a fault not within a zone of protection (other than operation as backup protection for a fault in an adjacent zone that is not cleared within a specified time for the protection for that zone). Any unintentional Protection System operation when no fault or other abnormal condition has occurred unrelated to on-site maintenance and testing activity.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Native Load [Archive]		2/8/2005	3/16/2007	The end-use customers that the Load-Serving Entity is obligated to serve.
Near-Term Transmission Planning Horizon [Archive]		1/24/2011	11/17/2011	The transmission planning period that covers Year One through five.
Net Actual Interchange [Archive]		2/8/2005	3/16/2007	The algebraic sum of all metered interchange over all interconnections between two physically Adjacent Balancing Authority Areas.
Net Energy for Load [Archive]		2/8/2005	3/16/2007	Net Balancing Authority Area generation, plus energy received from other Balancing Authority Areas, less energy delivered to Balancing Authority Areas through interchange. It includes Balancing Authority Area losses but excludes energy required for storage at energy storage facilities.
Net Interchange Schedule [Archive]		2/8/2005	3/16/2007	The algebraic sum of all Interchange Schedules with each Adjacent Balancing Authority.
Net Scheduled Interchange [Archive]		2/8/2005	3/16/2007	The algebraic sum of all Interchange Schedules across a given path or between Balancing Authorities for a given period or instant in time.
Network Integration Transmission Service [Archive]		2/8/2005	3/16/2007	Service that allows an electric transmission customer to integrate, plan, economically dispatch and regulate its network reserves in a manner comparable to that in which the Transmission Owner serves Native Load customers.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Non-Consequential Load Loss [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/15)	Non-Interruptible Load loss that does not include: (1) Consequential Load Loss, (2) the response of voltage sensitive Load, or (3) Load that is disconnected from the System by end-user equipment.
Non-Firm Transmission Service [Archive]		2/8/2005	3/16/2007	Transmission service that is reserved on an as-available basis and is subject to curtailment or interruption.
Non-Spinning Reserve [Archive]		2/8/2005	3/16/2007	<ol style="list-style-type: none"> 1. That generating reserve not connected to the system but capable of serving demand within a specified time. 2. Interruptible load that can be removed from the system in a specified time.
Normal Clearing [Archive]		11/1/2006	12/27/2007	A protection system operates as designed and the fault is cleared in the time normally expected with proper functioning of the installed protection systems.
Normal Rating [Archive]		2/8/2005	3/16/2007	The rating as defined by the equipment owner that specifies the level of electrical loading, usually expressed in megawatts (MW) or other appropriate units that a system, facility, or element can support or withstand through the daily demand cycles without loss of equipment life.
Nuclear Plant Generator Operator [Archive]		5/2/2007	10/16/2008	Any Generator Operator or Generator Owner that is a Nuclear Plant Licensee responsible for operation of a nuclear facility licensed to produce commercial power.
Nuclear Plant Off-site Power Supply (Off-site Power) [Archive]		5/2/2007	10/16/2008	The electric power supply provided from the electric system to the nuclear power plant distribution system as required per the nuclear power plant license.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Nuclear Plant Licensing Requirements [Archive]	NPLRs	5/2/2007	10/16/2008	Requirements included in the design basis of the nuclear plant and statutorily mandated for the operation of the plant, including nuclear power plant licensing requirements for: 1) Off-site power supply to enable safe shutdown of the plant during an electric system or plant event; and 2) Avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.
Nuclear Plant Interface Requirements [Archive]	NPIRs	5/2/2007	10/16/2008	The requirements based on NPLRs and Bulk Electric System requirements that have been mutually agreed to by the Nuclear Plant Generator Operator and the applicable Transmission Entities.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Off-Peak [Archive]		2/8/2005	3/16/2007	Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of lower electrical demand.
On-Peak [Archive]		2/8/2005	3/16/2007	Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of higher electrical demand.
Open Access Same Time Information Service [Archive]	OASIS	2/8/2005	3/16/2007	An electronic posting system that the Transmission Service Provider maintains for transmission access data and that allows all transmission customers to view the data simultaneously.
Open Access Transmission Tariff [Archive]	OATT	2/8/2005	3/16/2007	Electronic transmission tariff accepted by the U.S. Federal Energy Regulatory Commission requiring the Transmission Service Provider to furnish to all shippers with non-discriminating service comparable to that provided by Transmission Owners to themselves.
Operating Plan [Archive]		2/7/2006	3/16/2007	A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Operating Procedure [Archive]		2/7/2006	3/16/2007	A document that identifies specific steps or tasks that should be taken by one or more specific operating positions to achieve specific operating goal(s). The steps in an Operating Procedure should be followed in the order in which they are presented, and should be performed by the position(s) identified. A document that lists the specific steps for a system operator to take in removing a specific transmission line from service is an example of an Operating Procedure.
Operating Process [Archive]		2/7/2006	3/16/2007	A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon Real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.
Operating Reserve [Archive]		2/8/2005	3/16/2007	That capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages and local area protection. It consists of spinning and non-spinning reserve.
Operating Reserve – Spinning [Archive]		2/8/2005	3/16/2007	The portion of Operating Reserve consisting of: <ul style="list-style-type: none"> • Generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Operating Reserve – Supplemental [Archive]		2/8/2005	3/16/2007	The portion of Operating Reserve consisting of: <ul style="list-style-type: none"> • Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.
Operating Voltage [Archive]		2/7/2006	3/16/2007	The voltage level by which an electrical system is designated and to which certain operating characteristics of the system are related; also, the effective (root-mean-square) potential difference between any two conductors or between a conductor and the ground. The actual voltage of the circuit may vary somewhat above or below this value.
Operational Planning Analysis [Archive]		10/17/2008	3/17/2011	An analysis of the expected system conditions for the next day's operation. (That analysis may be performed either a day ahead or as much as 12 months ahead.) Expected system conditions include things such as load forecast(s), generation output levels, and known system constraints (transmission facility outages, generator outages, equipment limitations, etc.).
Operations Support Personnel [Archive]		2/6/2014		Individuals who perform current day or next day outage coordination or assessments, or who determine SOLs, IROLs, or operating nomograms, ¹ in direct support of Real-time operations of the Bulk Electric System.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Outage Transfer Distribution Factor [Archive]	OTDF	8/22/2008	11/24/2009	In the post-contingency configuration of a system under study, the electric Power Transfer Distribution Factor (PTDF) with one or more system Facilities removed from service (outaged).
Overlap Regulation Service [Archive]		2/8/2005	3/16/2007	A method of providing regulation service in which the Balancing Authority providing the regulation service incorporates another Balancing Authority's actual interchange, frequency response, and schedules into providing Balancing Authority's AGC/ACE equation.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Participation Factors [Archive]		8/22/2008	11/24/2009	A set of dispatch rules such that given a specific amount of load to serve, an approximate generation dispatch can be determined. To accomplish this, generators are assigned a percentage that they will contribute to serve load.
Peak Demand [Archive]		2/8/2005	3/16/2007	<ol style="list-style-type: none"> 1. The highest hourly integrated Net Energy For Load within a Balancing Authority Area occurring within a given period (e.g., day, month, season, or year). 2. The highest instantaneous demand within the Balancing Authority Area.
Performance-Reset Period [Archive]		2/7/2006	3/16/2007	The time period that the entity being assessed must operate without any violations to reset the level of non compliance to zero.
Physical Access Control Systems [Archive]	PACS	11/26/12	11/22/2013 (Becomes effective 4/1/16)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter [Archive]	PSP	5/2/2006	1/18/2008 (Becomes inactive 3/31/16)	The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.
Physical Security Perimeter [Archive]	PSP	11/26/12	11/22/2013 (Becomes effective 4/1/16)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Planning Assessment [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/15)	Documented evaluation of future Transmission System performance and Corrective Action Plans to remedy identified deficiencies.
Planning Authority [Archive]	PA	2/8/2005	3/16/2007	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
Planning Coordinator [Archive]	PC	8/22/2008	11/24/2009	See Planning Authority.
Point of Delivery [Archive]	POD	2/8/2005	3/16/2007	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction leaves or a Load-Serving Entity receives its energy.
Point of Receipt [Archive]	POR	2/8/2005	3/16/2007	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a Generator delivers its output.
Point to Point Transmission Service [Archive]	PTP	2/8/2005	3/16/2007	The reservation and transmission of capacity and energy on either a firm or non-firm basis from the Point(s) of Receipt to the Point(s) of Delivery.
Postback [Archive]		08/22/2008	Not approved; Modification directed 11/24/09	Positive adjustments to ATC or AFC as defined in Business Practices. Such Business Practices may include processing of redirects and unscheduled service.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Power Transfer Distribution Factor [Archive]	PTDF	08/22/2008	11/24/2009	In the pre-contingency configuration of a system under study, a measure of the responsiveness or change in electrical loadings on transmission system Facilities due to a change in electric power transfer from one area to another, expressed in percent (up to 100%) of the change in power transfer
Pro Forma Tariff [Archive]		2/8/2005	3/16/2007	Usually refers to the standard OATT and/or associated transmission rights mandated by the U.S. Federal Energy Regulatory Commission Order No. 888.
Protected Cyber Assets [Archive]	PCA	11/26/12	11/22/2013 (Becomes effective 4/1/16)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Protection System [Archive]		2/7/2006	3/17/2007 retired 4/1/2013	Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System [Archive] [Implementation Plan]		11/19/2010	2/3/2012 (Became effective on 4/1/13)	Protection System – <ul style="list-style-type: none"> • Protective relays which respond to electrical quantities, • Communications systems necessary for correct operation of protective functions • Voltage and current sensing devices providing inputs to protective relays, • Station dc supply associated with protective functions (including batteries, battery chargers, and non-battery-based dc supply), and • Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System Maintenance Program [Archive]	PSMP	11/7/2012	12/19/2013 (Becomes effective 4/1/2015)	An ongoing program by which Protection System components are kept in working order and proper operation of malfunctioning components is restored. A maintenance program for a specific component includes one or more of the following activities: Verify — Determine that the component is functioning correctly. Monitor — Observe the routine in-service operation of the component. Test — Apply signals to a component to observe functional performance or output behavior, or to diagnose problems. Inspect — Examine for signs of component failure, reduced performance or degradation. Calibrate — Adjust the operating threshold or measurement accuracy of a measuring element to meet the intended performance requirement.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System Maintenance Program [Archive]	PSMP	11/7/2013		An ongoing program by which Protection System and automatic reclosing components are kept in working order and proper operation of malfunctioning components is restored. A maintenance program for a specific component includes one or more of the following activities: Verify — Determine that the component is functioning correctly. Monitor — Observe the routine in-service operation of the component. Test — Apply signals to a component to observe functional performance or output behavior, or to diagnose problems. Inspect — Examine for signs of component failure, reduced performance or degradation. Calibrate — Adjust the operating threshold or measurement accuracy of a measuring element to meet the intended performance requirement.
Pseudo-Tie [Archive]		2/8/2005	3/16/2007	A telemetered reading or value that is updated in real time and used as a “virtual” tie line flow in the AGC/ACE equation but for which no physical tie or energy metering actually exists. The integrated value is used as a metered MWh value for interchange accounting purposes.
Purchasing-Selling Entity [Archive]	PSE	2/8/2005	3/16/2007	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Ramp Rate or Ramp [Archive]		2/8/2005	3/16/2007	(Schedule) The rate, expressed in megawatts per minute, at which the interchange schedule is attained during the ramp period. (Generator) The rate, expressed in megawatts per minute, that a generator changes its output.
Rated Electrical Operating Conditions [Archive]		2/7/2006	3/16/2007	The specified or reasonably anticipated conditions under which the electrical system or an individual electrical circuit is intend/designed to operate
Rating [Archive]		2/8/2005	3/16/2007	The operational limits of a transmission system element under a set of specified conditions.
Rated System Path Methodology [Archive]		08/22/2008	11/24/2009	The Rated System Path Methodology is characterized by an initial Total Transfer Capability (TTC), determined via simulation. Capacity Benefit Margin, Transmission Reliability Margin, and Existing Transmission Commitments are subtracted from TTC, and Postbacks and counterflows are added as applicable, to derive Available Transfer Capability. Under the Rated System Path Methodology, TTC results are generally reported as specific transmission path capabilities.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reactive Power [Archive]		2/8/2005	3/16/2007	The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar).
Real Power [Archive]		2/8/2005	3/16/2007	The portion of electricity that supplies energy to the load.
Reallocation [Archive]		2/8/2005	3/16/2007	The total or partial curtailment of Transactions during TLR Level 3a or 5a to allow Transactions using higher priority to be implemented.
Real-time [Archive]		2/7/2006	3/16/2007	Present time as opposed to future time. (From Interconnection Reliability Operating Limits standard.)
Real-time Assessment [Archive]		10/17/2008	3/17/2011	An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data
Receiving Balancing Authority [Archive]		2/8/2005	3/16/2007	The Balancing Authority importing the Interchange.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Regional Reliability Organization [Archive]	RRO	2/8/2005	3/16/2007	<ol style="list-style-type: none"> 1. An entity that ensures that a defined area of the Bulk Electric System is reliable, adequate and secure. 2. A member of the North American Electric Reliability Council. The Regional Reliability Organization can serve as the Compliance Monitor.
Regional Reliability Plan [Archive]		2/8/2005	3/16/2007	The plan that specifies the Reliability Coordinators and Balancing Authorities within the Regional Reliability Organization, and explains how reliability coordination will be accomplished.
Regulating Reserve [Archive]		2/8/2005	3/16/2007	An amount of reserve responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin.
Regulation Reserve Sharing Group [Archive]		8/15/2013		A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply the Regulating Reserve required for all member Balancing Authorities to use in meeting applicable regulating standards.
Regulation Service [Archive]		2/8/2005	3/16/2007	The process whereby one Balancing Authority contracts to provide corrective response to all or a portion of the ACE of another Balancing Authority. The Balancing Authority providing the response assumes the obligation of meeting all applicable control criteria as specified by NERC for itself and the Balancing Authority for which it is providing the Regulation Service.
Reliability Adjustment RFI [Archive]		10/29/2008	12/17/2009	Request to modify an Implemented Interchange Schedule for reliability purposes.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reliability Coordinator [Archive]	RC	2/8/2005	3/16/2007	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
Reliability Coordinator Area [Archive]		2/8/2005	3/16/2007	The collection of generation, transmission, and loads within the boundaries of the Reliability Coordinator. Its boundary coincides with one or more Balancing Authority Areas.
Reliability Coordinator Information System [Archive]	RCIS	2/8/2005	3/16/2007	The system that Reliability Coordinators use to post messages and share operating information in real time.
Reliability Directive [Archive]		8/16/2012		A communication initiated by a Reliability Coordinator, Transmission Operator, or Balancing Authority where action by the recipient is necessary to address an Emergency or Adverse Reliability Impact.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reliability Standard [Archive]		5/9/2013	7/9/2013	A requirement, approved by the United States Federal Energy Regulatory Commission under this Section 215 of the Federal Power Act, or approved or recognized by an applicable governmental authority in other jurisdictions, to provide for reliable operation [Reliable Operation] of the bulk-power system [Bulk-Power System]. The term includes requirements for the operation of existing bulk-power system [Bulk-Power System] facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation [Reliable Operation] of the bulk-power system [Bulk-Power System], but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.
Reliable Operation [Archive]		5/9/2013	7/9/2013	Operating the elements of the bulk-power system [Bulk-Power System] within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.
Remedial Action Scheme [Archive]	RAS	2/8/2005	3/16/2007	See "Special Protection System"

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reportable Cyber Security Incident [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/16)	A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.
Reportable Disturbance [Archive]		2/8/2005	3/16/2007	Any event that causes an ACE change greater than or equal to 80% of a Balancing Authority's or reserve sharing group's most severe contingency. The definition of a reportable disturbance is specified by each Regional Reliability Organization. This definition may not be retroactively adjusted in response to observed performance.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE [Archive]		8/15/2013		<p>The scan rate values of a Balancing Authority’s Area Control Error (ACE) measured in MW, which includes the difference between the Balancing Authority’s Net Actual Interchange and its Net Scheduled Interchange, plus its Frequency Bias obligation, plus any known meter error. In the Western Interconnection, Reporting ACE includes Automatic Time Error Correction (ATEC).</p> <p>Reporting ACE is calculated as follows:</p> $\text{Reporting ACE} = (\text{NI}_A - \text{NI}_S) - 10B (F_A - F_S) - I_{ME}$ <p>Reporting ACE is calculated in the Western Interconnection as follows:</p> $\text{Reporting ACE} = (\text{NI}_A - \text{NI}_S) - 10B (F_A - F_S) - I_{ME} + I_{ATEC}$ <p>Where:</p> <p>NI_A (Actual Net Interchange) is the algebraic sum of actual megawatt transfers across all Tie Lines and includes Pseudo-Ties. Balancing Authorities directly connected via asynchronous ties to another Interconnection may include or exclude megawatt transfers on those Tie lines in their actual interchange, provided they are implemented in the same manner for Net Interchange Schedule.</p> <p>NI_S (Scheduled Net Interchange) is the algebraic sum of all scheduled megawatt transfers, including Dynamic Schedules, with adjacent Balancing Authorities, and taking into account the effects of schedule ramps. Balancing Authorities directly connected via asynchronous ties to another Interconnection may include or exclude megawatt transfers on those Tie Lines in their scheduled Interchange, provided they are implemented in the same manner for Net</p>

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE (Continued)				<p>Interchange Actual.</p> <p>B (Frequency Bias Setting) is the Frequency Bias Setting (in negative MW/0.1 Hz) for the Balancing Authority.</p> <p>10 is the constant factor that converts the frequency bias setting units to MW/Hz.</p> <p>F_A (Actual Frequency) is the measured frequency in Hz.</p> <p>F_S (Scheduled Frequency) is 60.0 Hz, except during a time correction.</p> <p>I_{ME} (Interchange Meter Error) is the meter error correction factor and represents the difference between the integrated hourly average of the net interchange actual (NIA) and the cumulative hourly net Interchange energy measurement (in megawatt-hours).</p> <p>I_{A TEC} (Automatic Time Error Correction) is the addition of a component to the ACE equation for the Western Interconnection that modifies the control point for the purpose of continuously paying back Primary Inadvertent Interchange to correct accumulated time error. Automatic Time Error Correction is only applicable in the Western Interconnection.</p> $I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)^*H}$ <p>when operating in Automatic Time Error Correction control mode.</p> <p>I_{A TEC} shall be zero when operating in any other AGC mode.</p> <ul style="list-style-type: none"> • Y = B / BS. • H = Number of hours used to payback Primary Inadvertent Interchange energy. The value of H is set to 3. • BS = Frequency Bias for the Interconnection (MW / 0.1 Hz).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE (Continued)				<ul style="list-style-type: none"> Primary Inadvertent Interchange (PII_{hourly}) is $(1-Y) * (II_{actual} - B * \Delta TE/6)$ II_{actual} is the hourly Inadvertent Interchange for the last hour. ΔTE is the hourly change in system Time Error as distributed by the Interconnection Time Monitor. Where: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - (t) * (TE_{offset})$ TD_{adj} is the Reliability Coordinator adjustment for differences with Interconnection Time Monitor control center clocks. t is the number of minutes of Manual Time Error Correction that occurred during the hour. TE_{offset} is 0.000 or +0.020 or -0.020. PII_{accum} is the Balancing Authority's accumulated PII_{hourly} in MWh. An On-Peak and Off-Peak accumulation accounting is required. <p>Where: $PII_{accum}^{on/off\ peak} = \text{last period's } PII_{accum}^{on/off\ peak} + PII_{hourly}$ </p> <p>All NERC Interconnections with multiple Balancing Authorities operate using the principles of Tie-line Bias (TLB) Control and require the use of an ACE equation similar to the Reporting ACE defined above. Any modification(s) to this specified Reporting ACE equation that is(are) implemented for all BAs on an Interconnection and is(are) consistent with the following four principles will provide a valid alternative Reporting ACE equation</p>

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE (Continued)				<p>consistent with the measures included in this standard.</p> <ol style="list-style-type: none"> 1. All portions of the Interconnection are included in one area or another so that the sum of all area generation, loads and losses is the same as total system generation, load and losses. 2. The algebraic sum of all area Net Interchange Schedules and all Net Interchange actual values is equal to zero at all times. 3. The use of a common Scheduled Frequency FS for all areas at all times. 4. The absence of metering or computational errors. (The inclusion and use of the IME term to account for known metering or computational errors.)
Request for Interchange [Archive]	RFI	5/2/2006	3/16/2007	A collection of data as defined in the NAESB RFI Datasheet, to be submitted to the Interchange Authority for the purpose of implementing bilateral Interchange between a Source and Sink Balancing Authority.
Reserve Sharing Group [Archive]	RSG	2/8/2005	3/16/2007	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply operating reserves required for each Balancing Authority's use in recovering from contingencies within the group. Scheduling energy from an Adjacent Balancing Authority to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., ten minutes). If the transaction is ramped in quicker (e.g., between zero and ten minutes) then, for the purposes of Disturbance Control Performance, the Areas become a Reserve Sharing Group.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reserve Sharing Group Reporting ACE [Archive]		8/15/2013		At any given time of measurement for the applicable Reserve Sharing Group, the algebraic sum of the Reporting ACEs (or equivalent as calculated at such time of measurement) of the Balancing Authorities participating in the Reserve Sharing Group at the time of measurement.
Resource Planner [Archive]	RP	2/8/2005	3/16/2007	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
Response Rate [Archive]		2/8/2005	3/16/2007	The Ramp Rate that a generating unit can achieve under normal operating conditions expressed in megawatts per minute (MW/Min).
Right-of-Way [Archive]	ROW	2/7/2006	3/16/2007	A corridor of land on which electric lines may be located. The Transmission Owner may own the land in fee, own an easement, or have certain franchise, prescription, or license rights to construct and maintain lines.
Right-of-Way [Archive]	ROW	11/3/2011	3/21/2013 (Becomes inactive 6/30/14)	The corridor of land under a transmission line(s) needed to operate the line(s). The width of the corridor is established by engineering or construction standards as documented in either construction documents, pre-2007 vegetation maintenance records, or by the blowout standard in effect when the line was built. The ROW width in no case exceeds the Transmission Owner's legal rights but may be less based on the aforementioned criteria.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Right-of-Way [Archive]	ROW	5/9/12	(Becomes effective 7/1/14)	The corridor of land under a transmission line(s) needed to operate the line(s). The width of the corridor is established by engineering or construction standards as documented in either construction documents, pre-2007 vegetation maintenance records, or by the blowout standard in effect when the line was built. The ROW width in no case exceeds the applicable Transmission Owner's or applicable Generator Owner's legal rights but may be less based on the aforementioned criteria.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Scenario [Archive]		2/7/2006	3/16/2007	Possible event.
Schedule [Archive]		2/8/2005	3/16/2007	(Verb) To set up a plan or arrangement for an Interchange Transaction. (Noun) An Interchange Schedule.
Scheduled Frequency [Archive]		2/8/2005	3/16/2007	60.0 Hertz, except during a time correction.
Scheduling Entity [Archive]		2/8/2005	3/16/2007	An entity responsible for approving and implementing Interchange Schedules.
Scheduling Path [Archive]		2/8/2005	3/16/2007	The Transmission Service arrangements reserved by the Purchasing-Selling Entity for a Transaction.
Sending Balancing Authority [Archive]		2/8/2005	3/16/2007	The Balancing Authority exporting the Interchange.
Sink Balancing Authority [Archive]		2/8/2005	3/16/2007	The Balancing Authority in which the load (sink) is located for an Interchange Transaction. (This will also be a Receiving Balancing Authority for the resulting Interchange Schedule.)
Source Balancing Authority [Archive]		2/8/2005	3/16/2007	The Balancing Authority in which the generation (source) is located for an Interchange Transaction. (This will also be a Sending Balancing Authority for the resulting Interchange Schedule.)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Special Protection System (Remedial Action Scheme) [Archive]	SPS	2/8/2005	3/16/2007	An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) underfrequency or undervoltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS). Also called Remedial Action Scheme.
Spinning Reserve [Archive]		2/8/2005	3/16/2007	Unloaded generation that is synchronized and ready to serve additional demand.
Stability [Archive]		2/8/2005	3/16/2007	The ability of an electric system to maintain a state of equilibrium during normal and abnormal conditions or disturbances.
Stability Limit [Archive]		2/8/2005	3/16/2007	The maximum power flow possible through some particular point in the system while maintaining stability in the entire system or the part of the system to which the stability limit refers.
Supervisory Control and Data Acquisition [Archive]	SCADA	2/8/2005	3/16/2007	A system of remote control and telemetry used to monitor and control the transmission system.
Supplemental Regulation Service [Archive]		2/8/2005	3/16/2007	A method of providing regulation service in which the Balancing Authority providing the regulation service receives a signal representing all or a portion of the other Balancing Authority's ACE.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Surge [Archive]		2/8/2005	3/16/2007	A transient variation of current, voltage, or power flow in an electric circuit or across an electric system.
Sustained Outage [Archive]		2/7/2006	3/16/2007	The deenergized condition of a transmission line resulting from a fault or disturbance following an unsuccessful automatic reclosing sequence and/or unsuccessful manual reclosing procedure.
System [Archive]		2/8/2005	3/16/2007	A combination of generation, transmission, and distribution components.
System Operating Limit [Archive]	SOL	2/8/2005	3/16/2007	The value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to: <ul style="list-style-type: none"> • Facility Ratings (Applicable pre- and post-Contingency equipment or facility ratings) • Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits) • Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) • System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits)
System Operator [Archive]		2/8/2005	3/16/2007	An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
System Operator [Archive]		2/6/2014		An individual at a Control Center of a Balancing Authority, Transmission Operator, or Reliability Coordinator, who operates or directs the operation of the Bulk Electric System in Real-time.
Telemetry [Archive]		2/8/2005	3/16/2007	The process by which measurable electrical quantities from substations and generating stations are instantaneously transmitted to the control center, and by which operating commands from the control center are transmitted to the substations and generating stations.
Thermal Rating [Archive]		2/8/2005	3/16/2007	The maximum amount of electrical current that a transmission line or electrical facility can conduct over a specified time period before it sustains permanent damage by overheating or before it sags to the point that it violates public safety requirements.
Tie Line [Archive]		2/8/2005	3/16/2007	A circuit connecting two Balancing Authority Areas.
Tie Line Bias [Archive]		2/8/2005	3/16/2007	A mode of Automatic Generation Control that allows the Balancing Authority to 1.) maintain its Interchange Schedule and 2.) respond to Interconnection frequency error.
Time Error [Archive]		2/8/2005	3/16/2007	The difference between the Interconnection time measured at the Balancing Authority(ies) and the time specified by the National Institute of Standards and Technology. Time error is caused by the accumulation of Frequency Error over a given period.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Time Error Correction [Archive]		2/8/2005	3/16/2007	An offset to the Interconnection’s scheduled frequency to return the Interconnection’s Time Error to a predetermined value.
TLR (Transmission Loading Relief) ⁵ Log [Archive]		2/8/2005	3/16/2007	Report required to be filed after every TLR Level 2 or higher in a specified format. The NERC IDC prepares the report for review by the issuing Reliability Coordinator. After approval by the issuing Reliability Coordinator, the report is electronically filed in a public area of the NERC Web site.
Total Flowgate Capability [Archive]	TFC	08/22/2008	11/24/2009	The maximum flow capability on a Flowgate, is not to exceed its thermal rating, or in the case of a flowgate used to represent a specific operating constraint (such as a voltage or stability limit), is not to exceed the associated System Operating Limit.
Total Transfer Capability [Archive]	TTC	2/8/2005	3/16/2007	The amount of electric power that can be moved or transferred reliably from one area to another area of the interconnected transmission systems by way of all transmission lines (or paths) between those areas under specified system conditions.
Transaction [Archive]		2/8/2005	3/16/2007	See Interchange Transaction.

⁵ NERC added the spelled out term for TLR Log for clarification purposes.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Transfer Capability [Archive]		2/8/2005	3/16/2007	The measure of the ability of interconnected electric systems to move or transfer power <i>in a reliable manner</i> from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is <i>not</i> generally equal to the transfer capability from "Area B" to "Area A."
Transfer Distribution Factor [Archive]		2/8/2005	3/16/2007	See Distribution Factor.
Transmission [Archive]		2/8/2005	3/16/2007	An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.
Transmission Constraint [Archive]		2/8/2005	3/16/2007	A limitation on one or more transmission elements that may be reached during normal or contingency system operations.
Transmission Customer [Archive]		2/8/2005	3/16/2007	<ol style="list-style-type: none"> 1. Any eligible customer (or its designated agent) that can or does execute a transmission service agreement or can or does receive transmission service. 2. Any of the following responsible entities: Generator Owner, Load-Serving Entity, or Purchasing-Selling Entity.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Transmission Line [Archive]		2/7/2006	3/16/2007	A system of structures, wires, insulators and associated hardware that carry electric energy from one point to another in an electric power system. Lines are operated at relatively high voltages varying from 69 kV up to 765 kV, and are capable of transmitting large quantities of electricity over long distances.
Transmission Operator [Archive]	TOP	2/8/2005	3/16/2007	The entity responsible for the reliability of its “local” transmission system, and that operates or directs the operations of the transmission facilities.
Transmission Operator Area [Archive]		08/22/2008	11/24/2009	The collection of Transmission assets over which the Transmission Operator is responsible for operating.
Transmission Owner [Archive]	TO	2/8/2005	3/16/2007	The entity that owns and maintains transmission facilities.
Transmission Planner [Archive]	TP	2/8/2005	3/16/2007	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
Transmission Reliability Margin [Archive]	TRM	2/8/2005	3/16/2007	The amount of transmission transfer capability necessary to provide reasonable assurance that the interconnected transmission network will be secure. TRM accounts for the inherent uncertainty in system conditions and the need for operating flexibility to ensure reliable system operation as system conditions change.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Transmission Reliability Margin Implementation Document [Archive]	TRMID	08/22/2008	11/24/2009	A document that describes the implementation of a Transmission Reliability Margin methodology, and provides information related to a Transmission Operator's calculation of TRM.
Transmission Service [Archive]		2/8/2005	3/16/2007	Services provided to the Transmission Customer by the Transmission Service Provider to move energy from a Point of Receipt to a Point of Delivery.
Transmission Service Provider [Archive]	TSP	2/8/2005	3/16/2007	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
Vegetation [Archive]		2/7/2006	3/16/2007	All plant material, growing or not, living or dead.
Vegetation Inspection [Archive]		2/7/2006	3/16/2007	The systematic examination of a transmission corridor to document vegetation conditions.
Vegetation Inspection [Archive]		11/3/2011	3/21/2013 (Becomes inactive 6/30/14)	The systematic examination of vegetation conditions on a Right-of-Way and those vegetation conditions under the Transmission Owner's control that are likely to pose a hazard to the line(s) prior to the next planned maintenance or inspection. This may be combined with a general line inspection.
Vegetation Inspection [Archive]		5/9/12	(Becomes effective 7/1/14)	The systematic examination of vegetation conditions on a Right-of-Way and those vegetation conditions under the applicable Transmission Owner's or applicable Generator Owner's control that are likely to pose a hazard to the line(s) prior to the next planned maintenance or inspection. This may be combined with a general line inspection.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Wide Area [Archive]		2/8/2005	3/16/2007	The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits.
Year One [Archive]		1/24/2011	11/17/2011	The first twelve month period that a Planning Coordinator or a Transmission Planner is responsible for assessing. For an assessment started in a given calendar year, Year One includes the forecasted peak Load period for one of the following two calendar years. For example, if a Planning Assessment was started in 2011, then Year One includes the forecasted peak Load period for either 2012 or 2013.

ERCOT Regional Definitions

The following terms were developed as regional definitions for the ERCOT region:

ERCOT Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Measurable Event [Archive]	FME	8/15/2013	1/16/2014 (Becomes effective 4/1/14)	<p>An event that results in a Frequency Deviation, identified at the BA's sole discretion, and meeting one of the following conditions:</p> <ul style="list-style-type: none"> i) a Frequency Deviation that has a pre-perturbation [the 16-second period of time before t(0)] average frequency to post-perturbation [the 32-second period of time starting 20 seconds after t(0)] average frequency absolute deviation greater than 100 mHz (the 100 mHz value may be adjusted by the BA to capture 30 to 40 events per year). <p>Or</p> <ul style="list-style-type: none"> ii) a cumulative change in generating unit/generating facility, DC tie and/or firm load pre-perturbation megawatt value to post-perturbation megawatt value absolute deviation greater than 550 MW (the 550 MW value may be adjusted by the BA to capture 30 to 40 events per year).
Governor [Archive]		8/15/2013	1/16/2014 (Becomes effective	The electronic, digital or mechanical device that implements Primary Frequency Response of generating units/generating facilities or other system elements.

ERCOT Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
			4/1/14)	
Primary Frequency Response [Archive]	PFR	8/15/2013	1/16/2014 (Becomes effective 4/1/14)	The immediate proportional increase or decrease in real power output provided by generating units/generating facilities and the natural real power dampening response provided by Load in response to system Frequency Deviations. This response is in the direction that stabilizes frequency.

NPCC Regional Definitions

The following definitions were developed for use in NPCC Regional Standards.

NPCC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Current Zero Time [Archive]		11/04/2010	10/20/2011	The time of the final current zero on the last phase to interrupt.
Generating Plant [Archive]		11/04/2010	10/20/2011	One or more generators at a single physical location whereby any single contingency can affect all the generators at that location.

ReliabilityFirst Regional Definitions

The following definitions were developed for use in ReliabilityFirst Regional Standards.

RFC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Resource Adequacy [Archive]		08/05/2009	03/17/2011	The ability of supply-side and demand-side resources to meet the aggregate electrical demand (including losses)
Net Internal Demand [Archive]		08/05/2009	03/17/2011	Total of all end-use customer demand and electric system losses within specified metered boundaries, less Direct Control Management and Interruptible Demand
Peak Period [Archive]		08/05/2009	03/17/2011	A period consisting of two (2) or more calendar months but less than seven (7) calendar months, which includes the period during which the responsible entity's annual peak demand is expected to occur
Wind Generating Station [Archive]		11/03/2011		A collection of wind turbines electrically connected together and injecting energy into the grid at one point, sometimes known as a "Wind Farm."
Year One [Archive]		08/05/2009	03/17/2011	The planning year that begins with the upcoming annual Peak Period

WECC Regional Definitions

The following definitions were developed for use in WECC Regional Standards.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Area Control Error [†] [Archive]	ACE	3/12/2007	6/8/2007 (Becomes inactive 3/31/14)	Means the instantaneous difference between net actual and scheduled interchange, taking into account the effects of Frequency Bias including correction for meter error.
Automatic Generation Control [‡] [Archive]	AGC	3/12/2007	6/8/2007	Means equipment that automatically adjusts a Control Area's generation from a central location to maintain its interchange schedule plus Frequency Bias.
Automatic Time Error Correction [Archive]		3/26/2008	5/21/2009 (Becomes inactive 3/31/14)	A frequency control automatic action that a Balancing Authority uses to offset its frequency contribution to support the Interconnection's scheduled frequency.
Automatic Time Error Correction [Archive]		12/19/2012	10/16/2013 (Becomes effective 4/1/2014)	The addition of a component to the ACE equation that modifies the control point for the purpose of continuously paying back Primary Inadvertent Interchange to correct accumulated time error.
Average Generation [‡] [Archive]		3/12/2007	6/8/2007	Means the total MWh generated within the Balancing Authority Operator's Balancing Authority Area during the prior year divided by 8760 hours (8784 hours if the prior year had 366 days).
Business Day [‡] [Archive]		3/12/2007	6/8/2007	Means any day other than Saturday, Sunday, or a legal public holiday as designated in section 6103 of title 5, U.S. Code.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Commercial Operation [Archive]		10/29/2008	4/21/2011	Achievement of this designation indicates that the Generator Operator or Transmission Operator of the synchronous generator or synchronous condenser has received all approvals necessary for operation after completion of initial start-up testing.
Contributing Schedule [Archive]		2/10/2009	3/17/2011	A Schedule not on the Qualified Transfer Path between a Source Balancing Authority and a Sink Balancing Authority that contributes unscheduled flow across the Qualified Transfer Path.
Dependability-Based Misoperation [Archive]		10/29/2008	4/21/2011	Is the absence of a Protection System or RAS operation when intended. Dependability is a component of reliability and is the measure of a device's certainty to operate when required.
Disturbance [‡] [Archive]		3/12/2007	6/8/2007	Means (i) any perturbation to the electric system, or (ii) the unexpected change in ACE that is caused by the sudden loss of generation or interruption of load.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Extraordinary Contingency [‡] [Archive]		3/12/2007	6/8/2007	Shall have the meaning set out in Excuse of Performance, section B.4.c. language in section B.4.c: <i>means any act of God, actions by a non-affiliated third party, labor disturbance, act of the public enemy, war, insurrection, riot, fire, storm or flood, earthquake, explosion, accident to or breakage, failure or malfunction of machinery or equipment, or any other cause beyond the Reliability Entity's reasonable control; provided that prudent industry standards (e.g. maintenance, design, operation) have been employed; and provided further that no act or cause shall be considered an Extraordinary Contingency if such act or cause results in any contingency contemplated in any WECC Reliability Standard (e.g., the "Most Severe Single Contingency" as defined in the WECC Reliability Criteria or any lesser contingency).</i>
Frequency Bias [‡] [Archive]		3/12/2007	6/8/2007	Means a value, usually given in megawatts per 0.1 Hertz, associated with a Control Area that relates the difference between scheduled and actual frequency to the amount of generation required to correct the difference.
Functionally Equivalent Protection System [Archive]	FEPS	10/29/2008	4/21/2011	A Protection System that provides performance as follows: <ul style="list-style-type: none"> • Each Protection System can detect the same faults within the zone of protection and provide the clearing times and coordination needed to comply with all Reliability Standards. • Each Protection System may have different components and operating characteristics.
Functionally Equivalent RAS [Archive]	FERAS	10/29/2008	4/21/2011	A Remedial Action Scheme ("RAS") that provides the same performance as follows: <ul style="list-style-type: none"> • Each RAS can detect the same conditions and provide

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
				mitigation to comply with all Reliability Standards. <ul style="list-style-type: none"> • Each RAS may have different components and operating characteristics.
Generating Unit Capability [†] [Archive]		3/12/2007	6/8/2007	Means the MVA nameplate rating of a generator.
Non-spinning Reserve [†] [Archive]		3/12/2007	6/8/2007	Means that Operating Reserve not connected to the system but capable of serving demand within a specified time, or interruptible load that can be removed from the system in a specified time.
Normal Path Rating [†] [Archive]		3/12/2007	6/8/2007	Is the maximum path rating in MW that has been demonstrated to WECC through study results or actual operation, whichever is greater. For a path with transfer capability limits that vary seasonally, it is the maximum of all the seasonal values.
Operating Reserve [†] [Archive]		3/12/2007	6/8/2007	Means that capability above firm system demand required to provide for regulation, load-forecasting error, equipment forced and scheduled outages and local area protection. Operating Reserve consists of Spinning Reserve and Nonspinning Reserve.
Operating Transfer Capability Limit [†] [Archive]	OTC	3/12/2007	6/8/2007	Means the maximum value of the most critical system operating parameter(s) which meets: (a) precontingency criteria as determined by equipment loading capability and acceptable voltage conditions, (b) transient criteria as determined by equipment loading capability and acceptable voltage conditions, (c) transient performance criteria, and (d) post-contingency loading and voltage criteria.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Primary Inadvertent Interchange [Archive]		3/26/2008	5/21/2009	The component of area (n) inadvertent interchange caused by the regulating deficiencies of the area (n).
Qualified Controllable Device [Archive]		2/10/2009	3/17/2011	A controllable device installed in the Interconnection for controlling energy flow and the WECC Operating Committee has approved using the device for controlling the USF on the Qualified Transfer Paths.
Qualified Transfer Path [Archive]		2/10/2009	3/17/2011	A transfer path designated by the WECC Operating Committee as being qualified for WECC unscheduled flow mitigation.
Qualified Transfer Path Curtailment Event [Archive]		2/10/2009	3/17/2011	Each hour that a Transmission Operator calls for Step 4 or higher for one or more consecutive hours (See Attachment 1 IRO-006-WECC-1) during which the curtailment tool is functional.
Relief Requirement [Archive]		2/10/2009	3/17/2011	The expected amount of the unscheduled flow reduction on the Qualified Transfer Path that would result by curtailing each Sink Balancing Authority's Contributing Schedules by the percentages listed in the columns of WECC Unscheduled Flow Mitigation Summary of Actions Table in Attachment 1 WECC IRO-006-WECC-1.
Secondary Inadvertent Interchange [Archive]		3/26/2008	5/21/2009	The component of area (n) inadvertent interchange caused by the regulating deficiencies of area (i).
Security-Based Misoperation		10/29/2008	4/21/2011	A Misoperation caused by the incorrect operation of a Protection System or RAS. Security is a component of

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
[Archive]				reliability and is the measure of a device’s certainty not to operate falsely.
Spinning Reserve [†] [Archive]		3/12/2007	6/8/2007	Means unloaded generation which is synchronized and ready to serve additional demand. It consists of Regulating reserve and Contingency reserve (as each are described in Sections B.a.i and ii).
Transfer Distribution Factor [Archive]	TDF	2/10/2009	3/17/2011	The percentage of USF that flows across a Qualified Transfer Path when an Interchange Transaction (Contributing Schedule) is implemented. [See the WECC Unscheduled Flow Mitigation Summary of Actions Table (Attachment 1 WECC IRO-006-WECC-1).]
WECC Table 2 [†] [Archive]		3/12/2007	6/8/2007	Means the table maintained by the WECC identifying those transfer paths monitored by the WECC regional Reliability coordinators. As of the date set out therein, the transmission paths identified in Table 2 are as listed in Attachment A to this Standard.

Endnotes

[†] FERC approved the WECC Tier One Reliability Standards in the Order Approving Regional Reliability Standards for the Western Interconnection and Directing Modifications, 119 FERC ¶ 61,260 (June 8, 2007). In that Order, FERC directed WECC to address the inconsistencies between the regional definitions and the NERC Glossary in developing permanent replacement standards. The replacement standards designed to address the shortcomings were filed with FERC in 2009.

Exhibit B

**Informational Summary of Each Reliability Standard Applicable to Nova Scotia,
Approved by FERC in Fourth Quarter 2013**

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

BAL-001-1- To maintain Interconnection steady-state frequency within defined limits by balancing real power demand and supply in real-time.

Applicability:

- Balancing Authorities

Reliability Standard BAL-001-1 includes four requirements and Appendix 1.

On August 20, 2013, NERC submitted a petition for approval of BAL-001-1 2 to the Federal Energy Regulatory Commission (“FERC”) and on October 16, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

CIP-002-5.1- To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-002-5.1 includes two requirements.

On January 31, 2013, NERC submitted a petition for approval of CIP-002-5.1 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

EXHIBIT B: Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in Fourth Quarter 2013

CIP-003-5- To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-003-5 includes four requirements.

On January 31, 2013, NERC submitted a petition for approval of CIP-003-5 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

CIP-004-5.1- To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-004-5.1 includes five requirements and several tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-004-5.1 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

CIP-005-5- To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-005-5 includes two requirements and several tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-005-5 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

CIP-006-5- To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - Generator Operators
 - Generator Owners
 - Interchange Coordinators or Interchange Authorities
 - Reliability Coordinators
 - Transmission Operators
 - Transmission Owners

Reliability Standard CIP-006-5 includes three requirements and several tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-006-5 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

CIP-007-5- To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-007-5 includes five requirements and several tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-007-5 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

CIP-008-5- To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - Generator Operators
 - Generator Owners
 - Interchange Coordinators or Interchange Authorities
 - Reliability Coordinators
 - Transmission Operators
 - Transmission Owners

Reliability Standard CIP-008-5 includes three requirements and several tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-008-5 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

EXHIBIT B: Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in Fourth Quarter

CIP-009-5- To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-009-5 includes three requirements and several tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-009-5 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

EXHIBIT B: Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in Fourth Quarter

CIP-010-1- To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-010-1 includes three requirements and several tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-010-1 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

EXHIBIT B: Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in Fourth Quarter

CIP-011-1- To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Applicability:

- Balancing Authorities
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection of restoration of BES:
 - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more
- Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- Generator Operators
- Generator Owners
- Interchange Coordinators or Interchange Authorities
- Reliability Coordinators
- Transmission Operators
- Transmission Owners

Reliability Standard CIP-011-1 includes two requirements and two tables.

On January 31, 2013, NERC submitted a petition for approval of CIP-011-1 to the Federal Energy Regulatory Commission (“FERC”) and on November 22, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

PRC-005-2- To document and implement programs for the maintenance of all Protection Systems affecting the reliability of the Bulk Electric System (BES) so that these Protection Systems are kept in working order.

Applicability:

- Transmission Owners
- Generator Owners
- Distribution Providers

Reliability Standard PRC-005-2 includes five requirements and several tables.

On February 26, 2013, NERC submitted a petition for approval of PRC-005-2 to the Federal Energy Regulatory Commission (“FERC”) and on December 19, 2013, FERC approved the standard.

**EXHIBIT B: Informational Summary of Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2013**

TPL-001-4- Establish Transmission system planning performance requirements within the planning horizon to develop a Bulk Electric System (BES) that will operate reliably over a broad spectrum of System conditions and following a wide range of probable Contingencies.

Applicability:

- Planning Coordinator
- Transmission Planner

Reliability Standard TPL-001-4 includes eight requirements and Table 1. The revised standard contains a series of planning events and describes system performance requirements in Table 1 for a range of potential system contingencies required to be evaluated by the planner. Table 1 includes three parts: Steady State & Stability Performance Planning Events, Steady State & Stability Performance Extreme Events, and Steady State & Stability Performance Footnotes. Table 1 categorizes the events as either “planning events” or “extreme events.” The proposed table lists seven contingency planning events that require steady-state and stability analysis as well as five extreme event contingencies.

On February 28, 2013, NERC submitted a petition for approval of TPL-001-4 to the Federal Energy Regulatory Commission (“FERC”) and on October 17, 2013, FERC approved the standard.