UNITED STATES OF AMERICA
Before the
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket Nos. RD09-7-000**

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO THE FEDERAL ENERGY REGULATORY COMMISSION'S SEPTEMBER 30, 2009 ORDER APPROVING REVISED RELIABILITY STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION AND REQUIRING COMPLIANCE FILING

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

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

December 29, 2009

TABLE OF CONTENTS

ATTACHMENTS:

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") respectfully submits this compliance filing in response to the Federal Energy Regulatory Commission's ("FERC") Order issued September 30, 2009[1] approving Version 2 of the Critical Infrastructure Protection ("CIP") Reliability Standards ("Version 2 CIP Order"). This filing includes:

1. A request for approval of Version 3 of the Critical Infrastructure Protection Reliability Standards ("Version 3 CIP Standards");[2]
2. A request for approval of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and the Implementation Plan for Version 3 of the Cyber Security Standards CIP-002-3 through CIP-009-3 ("Implementation Plan for Version 3") that addresses FERC's directives in the Version 2 CIP Order; and
3. An update of the timetable that reflects the plan to address the remaining FERC directives from Order No. 706.[3]

The Version 2 CIP Order approved the Version 2 CIP Reliability Standards and the CIP Version 2 Implementation Plan and directed NERC, as the Electric Reliability Organization ("ERO"), to develop certain modifications to the Version 2 CIP Reliability Standards and the associated Version 2 Implementation Plan, and to submit an updated timeline for addressing the remaining

[1] *North American Electric Reliability Corporation*, Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing, 128 FERC ¶ 61,291 (2009) ("Version 2 CIP Order").
[2] Version 3 of the CIP Standards is the same as Version 2 in all respects, except for the specific changes made to CIP-006-2 and CIP-008-2 to address the directives from the Version 2 CIP Order. NERC is resubmitting all CIP standards as Version 3 CIP standards for ease of reference.
[3] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

Order No. 706 directives. NERC was directed to respond to the directives in the Version 2 CIP Order within ninety days, or by December 29, 2009. This filing addresses FERC's directives.

The NERC Board of Trustees approved the Version 3 CIP Reliability Standards, the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and the Implementation Plan for Version 3 on December 16, 2009. NERC requests that FERC approve the proposed Version 3 Reliability Standards and make them effective in accordance with the effective date provisions set forth in the proposed Reliability Standards. NERC also requests that FERC approve the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and make it effective April 1, 2010, the same date the Version 2 CIP standards become effective.

Exhibit 1 to this filing sets forth the proposed Version 3 CIP Reliability Standards. **Exhibit 2** contains the complete development record of the proposed Reliability Standards. **Exhibit 3** contains the roster of the standard drafting team that developed the proposed Reliability Standards. **Exhibit 4a** contains the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. **Exhibit 4b** contains the Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3. **Exhibit 5** contains an update of the timetable that reflects the plan to address the remaining FERC directives from Order No. 706. **Exhibits 6a** and **6b** provide revisions to the Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") associated with the CIP Version 3 changes, and an updated complete listing of VRFs and VSLs, respectively.

NERC is also filing these proposed Reliability Standards and Implementation Plans with applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

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

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

* Persons to be included on FERC's service list are indicated with an asterisk. NERC requests waiver of FERC's rules and regulations to permit the inclusion of more than two people on the service list.

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

III. RESPONSES TO VERSION 2 CIP ORDER – COMPLIANCE ITEMS DUE DECEMBER 29, 2009

A. Version 3 CIP Standards

In the Version 2 CIP Order, FERC directed NERC to modify the Version 2 CIP Standards as follows:

Version 2 CIP Order, P 30:

> Pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop a modification to Reliability Standard CIP-006-2, through the NERC Reliability Standards development process, to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit, within 90 days from the date of this order ...

Version 2 CIP Order, P 38:

> Pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop a modification to Reliability Standard CIP-008-2, Requirement R1.6, through the NERC Reliability Standards development process, to remove the last sentence of CIP-008-2 Requirement R1.6.

NERC Response:

In accordance with FERC's directives in Paragraphs 30 and 38 of the Version 2 CIP Order, NERC hereby proposes for FERC approval a revised set of Version 3 CIP standards. The modifications to proposed CIP-006-3 and CIP-008-3 were developed using NERC's *Reliability Standards Development Procedure* and were approved by stakeholders through the NERC balloting process. While the modifications proposed in this filing pertain only to CIP-006 and CIP-008, NERC submits the full suite of CIP standards, CIP-002 through CIP-009 as Version 3 for ease of reference and to simplify applicable entities' understanding in determining the appropriate implementation date. In addition, new VRFs and VSLs are proposed for the modified requirements in CIP-006-3 and CIP-008-3. Conforming changes to the VSLs for CIP-005-3 and CIP-007-3 were deemed necessary in converting CIP-002-2 through CIP-009-2 into CIP-002-3 into CIP-009-3. These confirming changes are included in **Exhibit 6a and 6b for approval.** For those requirements not being modified in this filing, NERC requests FERC to carry forward the currently-approved Version 2 VRFs and VSLs to the Version 3 requirements.

1. Regulatory Framework

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

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

2. Basis for Approval of Proposed Reliability Standards

Section 39.5(a) of FERC's regulations requires the ERO to file with FERC for its approval each Reliability Standard that the ERO proposes to become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to be made effective. FERC has the regulatory responsibility to approve standards that protect the reliability of the bulk power system. In discharging its responsibility to review, approve, and enforce mandatory Reliability Standards, FERC is authorized to approve those proposed Reliability Standards that meet the criteria detailed by Congress:

> The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest.[5]

When evaluating proposed Reliability Standards, FERC is expected to give "due weight" to the technical expertise of the ERO. Order No. 672 provides guidance on the factors FERC will consider when determining whether proposed Reliability Standards meet the statutory criteria.[6]

3. Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC *Reliability Standards Development Procedure*, which is incorporated into the Rules of Procedure as Appendix 3A. In its ERO Certification Order, FERC found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in

[5] Section 215(d)(2) of the FPA, 16 U.S.C. § 824o(d)(2) (2000).
[6] See Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, FERC Stats. & Regs., ¶ 31,204 at PP 320-338 ("Order No. 672"), order on reh'g, FERC Stats. & Regs. ¶ 31,212 (2006) ("Order No. 672-A").

developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards.[7]

The development process is open to any person or entity with a legitimate interest in the reliability of the bulk power system. NERC considers the comments of all stakeholders and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard before its submission to FERC.

The proposed Reliability Standards set out in **Exhibit 1** have been developed and approved by industry stakeholders using NERC's *Reliability Standards Development Procedure*. They were approved by the NERC Board of Trustees on December 16, 2009.

4. Justification for Approval of Proposed Reliability Standards

In this filing, NERC is proposing Version 3 CIP Standards that are responsive to FERC's directives in the Version 2 CIP Order within the ninety-day delivery timeframe. No other changes are being proposed apart from those identified in the Version 2 CIP Order.

5. Summary of Reliability Standards Development Proceedings

Following the issuance of the Version 2 CIP Order, NERC initiated a new project, Project 2009-21 — Cyber Security Ninety-Day Response to address FERC's directives. The Standards Committee assigned the existing Cyber Security Order No. 706 standard drafting team to address the directives in the Version 2 CIP Order. The scope of the project included developing the changes to CIP-006-2 and CIP-008-2 as directed by FERC and developing conforming changes to CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, CIP-007-2, and CIP-009-2 to correct the cross references to CIP-006 and CIP-008 within the set of standards. Additionally, VRFs and VSLs are included for modified requirements in CIP-006-3 and CIP-008-3. The project scope also

[7] Order No. 672 at PP 268, 270.

included revising the CIP Version 2 Implementation Plan to address the matters specified in the Version 2 CIP Order. The Implementation Plan changes are discussed in Section III.B of this filing.

NERC posted the proposed Standards Authorization Request for Project 2009-21, proposed Version 3 CIP standards changes, associated VRFs and VSLs, the proposed Implementation Plan for the Version 3 CIP standards, and a revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for a 30-day industry comment period that concluded on November 12, 2009. There were 29 sets of comments received in response to the posting from more than 60 people in 40 different companies representing 8 of the 10 Industry Segments. In addition to comments regarding the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to be discussed in the following section, the team determined that changes to CIP-006-3 were necessary to more closely conform to the specific FERC directive.

As a result, whereas CIP-006-2, Requirement R1 requires the applicable entity to document, implement, and maintain a physical security plan that includes, in accordance with sub-requirement R1.6, "[c]ontinuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access," the proposed version of CIP-006-3, sub-requirement R1.6 has been expanded to the following:

> **R1.6** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
>
> **R1.6.1**. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
>
> **R1.6.2**. Continuous escorted access of visitors within the Physical Security Perimeter.

Additionally, in accordance with FERC's directive, NERC also proposes a revised CIP-008-3 standard that removes the last sentence of sub-requirement R1.6.

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

In order to meet the ninety-day response window, the NERC Standards Committee authorized deviations from the typical standards development process by commencing the pre-ballot review window and assembly of the ballot pool concurrent with the industry comment period. The ballot pool and pre-ballot review window began on October 27, 2009 and concluded on November 20, 2009. NERC held the initial ballot for the Version 3 CIP Standards, associated VRFs and VSLs, the Implementation Plan for the Version 3 CIP Standards, and the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities from November 20, 2009 through November 30, 2009. With 89.58 percent of the ballot pool participating, the proposed standards and associated documents achieved a weighted segment approval of 88.07 percent. There were 28 negative ballots where 17 comments were submitted with a negative ballot and 5 accompanying an affirmative ballot. No commenters addressed the changes proposed in CIP-008-3. However, several commented on the proposed CIP-006-3 modifications, including one commenter that disagreed with FERC's timeline for delivery of these changes. In the commenter's view, the changes were inconsequential to reliability and diverted scarce resources working on the substantive revisions to the CIP standards, as required by Order No. 706, in order to address FERC's directives in the Version 2 CIP Order.

The team clarified its intent in the response to the various comments but made no changes to the proposed standards as a result. NERC conducted the recirculation ballot from December 3, 2009 through December 14, 2009. With 93.33 percent of the ballot pool voting, the proposed standards and associated documents achieved a weighted segment approval of 85.55

percent. The NERC Board of Trustees approved the standards, VRFs and VSLs, the associated Version 3 CIP Standard Implementation Plan, and a revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities via conference call on December 16, 2009.

B. Revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Version 2 CIP Order, P 40:

> We reject the first document identified above, "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2," because it is unnecessary and causes confusion. For instance, this document discusses the proposed effective date of the Version 2 CIP Reliability Standards, but this discussion is unnecessary because each such Standard includes a provision describing its effective date. The first document also discusses the date by which "newly registered entities" must comply with the Version 2 CIP Reliability Standards. This document does not define "newly registered entities," but its statements appear consistent with the timeline for compliance set forth in Table 3 of the second document that applies to "Entities Registering in 2008 and Thereafter." We believe the first document is confusing since it is unclear how it relates to the second document. If NERC believes that information contained in this document is useful for explanatory purposes, NERC should incorporate the relevant information into the second implementation plan to create a single, comprehensive document.

Version 2 CIP Order, P 41:

> Considered alone, we find that the second document identified above, "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or their Successor Standards," (the Version 2 Implementation Plan or Version 2 plan) lacks clarity and could be open to multiple interpretations on some topics. Commission Staff prepared a document reflecting our concerns in this regard, which is attached to this order. We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order.

NERC Response:

First, a brief history of the CIP implementation plans is in order. FERC approved the

implementation plan that NERC proposed for Version 1 of the CIP Standards in Order No. 706.[8] That implementation plan provided for implementation of the CIP Version 1 Reliability Standards over a three-year period. It set out a proposed schedule for accomplishing the various tasks associated with compliance with the CIP Reliability Standards and gave a timeline, by calendar quarters, for completing various tasks and prescribed milestones for when a responsible entity must: (1) "begin work" to be compliant with a requirement; (2) "be substantially compliant" with a Requirement; (3) "be compliant" with a Requirement; and (4) "be auditably compliant" with a Requirement. According to the implementation plan, "auditably compliant" must be achieved in 2009 for certain Requirements by certain responsible entities, and in 2010 for others. The responsible entities were classified as Table 1, Table 2, Table 3, or Table 4 entities, with various implementation dates, depending on which functions they were registered for and whether or not they had previously been required to certify compliance with Urgent Action Cyber Standard 1200. All were to be auditably compliant by December 31, 2010.

When NERC filed Version 2 of the CIP Reliability Standards in May 2009, it also filed a revised implementation plan, in two documents. The first document, styled "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2," stated that when the Version 2 standards became effective, the Version 1 standards and the Version 1 implementation plan would be retired. The first part also repeated the effective date provision from each of the Version 2 CIP standards, namely, that the Version 2 standards become effective "on the first day of the third quarter after receiving regulatory approval." The Version 2 implementation plan also stated that responsible entities must comply with the Version 2 CIP standards "once the standards become effective."

[8] Order No. 706, P 86.

The second document filed in May 2009 was styled "Implementation Plan for Newly Identified Critical Cyber Assets or Newly Registered Entities for Cyber Security Standards CIP-003-1 through CIP-009-1 or Their Successor Standards." The purpose of the second document was to specify an implementation schedule for situations where an entity already subject to the CIP standards identified new critical cyber assets or where an entity was newly included on the NERC Compliance Registry (and thus was subject to CIP standards for the first time, specifically CIP-002 that required the use of a risk-based methodology for identifying Critical Cyber Assets).

In the Version 2 CIP Order, FERC rejected the first document as unnecessary, because it repeated the effective date provisions from each of the Version 2 CIP standards. NERC understands the effect of the Version 2 CIP Order in this regard is that responsible entities must be in compliance with Version 2 of the CIP standards as of April 1, 2010, the date those standards become effective. FERC found that the second document lacked clarity in several aspects and directed NERC to file a revised document that addressed the issues listed.

The revised Implementation Plan called for by the Version 2 CIP Order is presented in two documents in this filing. The first document, **Attachment 4a**, is styled "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities." It applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3. This document addresses the enumerated list of corrections and clarifications that were included with FERC's Version 2 CIP Order. NERC requests that FERC approve this implementation plan and make it effective on April 1, 2010, to coincide with the effective date of the CIP Version 2 standards.

The second document, styled as "Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3" (**Attachment 4b**), does a number of things, all in one

place. First, it states that prior versions of the CIP standards will be retired when the Version 3 CIP standards become effective. Second, it states that responsible entities must be compliant with Version 3 of the CIP standards on the date those standards become effective. Third, the document references the effective date provision in the Version 3 CIP standards, which states that the Version 3 CIP standards become effective on the first day of the third quarter following regulatory approval. By way of example, if FERC approves the Version 3 CIP standards before April 1, 2010, then the Version 3 CIP standards will become effective October 1, 2010. Responsible entities would then be required to be in compliance with the Version 3 CIP standards as of that date.[9] Fourth, the document explains that Newly Identified Critical Cyber Assets and Newly Registered Entities are covered by the "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities." Finally, the second document explains that the original implementation plan for the Version 1 CIP standards will, as a practical matter, end on December 31, 2010, because on that date all Table 1, 2, and 3 entities must be auditably compliant.

As of April 1, 2010, NERC envisions two Implementation Plans will be in effect – the Implementation Plan for Version 3, which effectively implements the FERC-approved Version 1 implementation plan dates for Table 1, Table 2, and Table 3 entities for Version 1, Version 2, or Version 3 standards, whichever are in effect; as well as the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. On December 31, 2010, when the Version 1 Implementation Plan implementation dates are, in practice, retired, only the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities will remain in effect.

[9] It is important to note that the only substantive changes from Version 2 to Version 3 occur in CIP-006 and CIP-008, in response to directives in the Version 2 CIP Order.

While FERC expressed concern over the usefulness of the Version 2 Implementation Plan document and directed that NERC incorporate the relevant information into the second document, NERC believes each document serves a useful purpose. Therefore, NERC chose to clarify the content of each document to remove the confusion noted in FERC's attachment to the Version 2 CIP Order. In addition to defining "newly registered entities," FERC identifies a list of 13 concerns in the attachment, designated "a" through "m," which NERC addresses in sequential order below. Following this discussion, a description of the development activities relative to the implementation plans is provided.

a. The Version 2 Implementation Plan states at page 1 that it identifies the schedule for becoming compliant with the requirements of CIP-003-2 through CIP-009-2 and their successor Standards "for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed." The use of the phrase "existing Implementation Plan" here and elsewhere on page 1 of the Version 2 Implementation Plan causes confusion as to whether the Version 1 Implementation Plan or the proposed plan is being referenced. We direct NERC to clarify that the "existing" implementation plan is the Version 1 Implementation Plan.

The reference to "existing Implementation Plan" has been clarified in the proposed revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. In the second paragraph on Page 1, NERC clarifies that the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities applies to Version 2 or Version 3 of the CIP standards for both: a) newly identified Critical Cyber Assets by existing Registered Entities after their Compliant milestone date has passed; and, b) newly Registered Entities, thus addressing two distinct scenarios for different types of entities.

The first scenario concerns entities that are already registered on the NERC Compliance Registry, and are therefore subject to compliance with NERC Reliability Standards. It is therefore assumed that these entities are already compliant with the requirements of CIP-002, have a risk-based methodology for identifying Critical Assets, and have identified any Critical

Cyber Assets associated with the identified Critical Assets. In this scenario, newly identified Critical Assets and/or newly identified Critical Cyber Assets are designated as a result of the application of the risk-based methodology in CIP-002, and as described in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. In this scenario, the entity must follow the timeline defined in Table 2 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to determine when it must be compliant with the requirements of CIP-003 through CIP-009.

The second scenario deals with a wholly new registered entity that has no history of registration on the NERC Compliance Registry under its existing or predecessor organization, and therefore has not previously been required to be compliant with the NERC Reliability Standards. Note that merged and acquired companies, and acquired assets are specifically discussed in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the context of the first scenario described in the previous paragraph.

When the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was originally submitted with the Version 2 CIP standards, there was no way of determining what the specific compliance dates for Version 2 would be, thus there was no specificity with regard to the compliance dates. Now that the Version 2 standards have been approved by FERC, Version 1 and Version 2 implementation dates are known, and have been included in the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. In order for the proposed Implementation Plan dates for Newly Identified Critical Cyber Assets and Newly Registered Entities to coincide with the April 1, 2010 effective date for Version 2 of the CIP standards, NERC requests that FERC approve this Implementation Plan to become effective on April 1, 2010.

b. The Version 2 Implementation Plan refers at page 3 several times to "this New Asset Implementation Plan." We direct NERC to delete or change this inaccurate reference.

NERC adds significantly more specificity to the various categories and milestones in the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities such that the objectionable term, "New Asset Implementation Plan" is not necessary and is deleted in the proposal included in this filing.

c. The Version 2 Implementation Plan refers at pages 3 and 4 several times to "an established CIP Compliance program as required by an existing Implementation Schedule." We direct NERC to clarify the meaning of "an established CIP Compliance program." In particular, we direct NERC to state whether a "CIP Compliance program" includes a program for complying with CIP-002 or is limited to a CIP compliance program for CIP-003 through CIP-009, as stated for Category 1 listed under the heading "Implementation Schedule" on page 1 of the Version 2 Implementation Plan. We also direct NERC to clarify the meaning of "an existing Implementation Schedule."

In footnote 3 on Page 2 of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, NERC clarifies the term "CIP compliance implementation program" to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC CIP Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All existing Registered Entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version-specific Implementation Plan. NERC clarifies that the applicable milestones for various categories of Registered Entities are governed by Tables 1, 2, and 3 of the CIP Version 1 standard implementation schedules. The Version 1 Implementation Plan therefore provides the applicable implementation dates for Table 1, Table 2, and Table 3 entities. This is described in more detail in the Implementation Plan for Version 3, included in **Exhibit 4b** to this filing.

The Version 2 CIP Order has set the implementation date for Version 2 of the CIP standards as April 1, 2010. For entities that registered on the NERC Compliance Registry after

April 2008, the implementation schedule for the Version 2 or Version 3 CIP standards, whichever are in effect, can be determined through Table 3 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. Accordingly, NERC requests that FERC approve the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities effective April 1, 2010, to coincide with the effective date of the CIP Version 2 standards.

To further add clarity to the implementation and enforcement schedules relative to Versions 1 and Version 2, NERC intends to update its 2010 Uniform Compliance Monitoring and Enforcement Program ("CMEP") Implementation Plan to account for the "effective date" of the Version 2 CIP standards of April 1, 2010 for all entities. When a compliance audit occurs, the Responsible Entity will be audited to the Version 1 CIP standards for the portion of the audit period prior to April 1, 2010 and to Version 2 for the remainder of the audit period after April 1, 2010. However, the compliance milestones (the "compliant" and "auditably compliant" dates) will remain set by the original Version 1 implementation plan: for Table 1 entities, the auditably compliant date is July 1, 2009 for 13 requirements and July 1, 2010 for the remaining requirements; for Table 2 entities, the auditably compliant date is July 1, 2009 for CIP-003, Requirement R2 and July 1, 2010 for all remaining requirements; and for Table 3 entities the auditably compliant date is December 31, 2009 for CIP-003, Requirement R2 and December 31, 2010 for all remaining requirements. In effect, the April 1, 2010 effective date determines the substance of the audits, but the original Version 1 Implementation Plan will continue to set the schedule for the audits.

d. We direct NERC to clarify whether the Version 2 Implementation Plan contemplates that the Version 1 Implementation Plan will be retired upon the effective date of the Version 2 CIP Reliability Standards. If not, we require further explanation as to how the Version 1 Implementation Plan will still be applicable. The revised plan should be clear which entities must continue to rely upon the Version 1 Implementation Plan, and to what extent in which circumstances.

NERC includes in this filing the Implementation Plan for Version 3, which explains that the implementation dates included in Version 1 of the Implementation Plan shall remain in effect for Table 1, Table 2, and Table 3 entities for compliance with Version 1, Version 2, and Version 3, whichever is in effect, until the implementation dates are in practice, retired on December 31, 2010. The last section of this document entitled, "Prior Version Implementation Plan Retirement," includes specific detail regarding the retirement of the Version 1 Implementation Plan Tables 1, 2, and 3 and concludes that as of December 31, 2010, the date on which Table 3 Registered Entities reach the Auditably Compliant state, the Version 1 Implementation Plan is no longer needed and will be retired. This aspect is also consistent with the process noted above that will be updated in the 2010 CMEP Implementation Plan. Table 4 of the Version 1 Implementation Plan deals with the treatment of newly Registered Entities. These entities are wholly included in Table 3 of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, submitted with this filing, that NERC is requesting FERC approve and make effective on April 1, 2010. After December 31, 2010, the only Implementation Plan in effect will be the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities submitted with this filing.

e. In the third paragraph of page 1, the Version 2 Implementation Plan refers to "some requirements" for which a Responsible Entity is expected to be Compliant upon the designation of the newly identified Critical Cyber Asset, stating that these instances are "annotated as '0'." We observe that the Version 2 Implementation Plan does not annotate any requirement as "0." We direct NERC to explain or delete this statement and to list each requirement for which a Responsible Entity is expected to be Compliant immediately upon designation of a newly identified Critical Cyber Asset.

NERC has deleted the incorrect annotation and has further described with greater specificity the compliance expectations for newly identified Critical Cyber Assets based on the various categories for identification. Table 1 provides a useful list of examples describing how to apply Table 2 for the various identification scenarios. Generally, there are no requirements in Table 2 for which a Responsible Entity is expected to be Compliant immediately upon designation of a newly identified Critical Cyber Asset. However, for a Responsible Entity with an existing CIP compliance implementation program for CIP-003 through CIP-009, the following conditions require compliance upon the commissioning of the asset:

- any asset identified as a Critical Asset with associated Critical Cyber Assets that comes on-line
- any existing Cyber Asset that is reconfigured to be within the Electronic Security Perimeter
- any new Cyber Asset added into a new or existing Electronic Security Perimeter
- any new Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter, or
- any planned modification or upgrade to an existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset.

f. In the third paragraph of page 1, the Version 2 Implementation Plan also refers to "other requirements" for which the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date, stating that these are annotated as "existing." We observe that Table 2 of the Version 2 Implementation Plan annotates the following requirements as "existing" for "Milestone Category 2": CIP-003-2, R1 through R3 and CIP-004-2 Requirement R1. We direct NERC to confirm whether these requirements are the only requirements annotated as "existing" in the Version 2 Implementation Plan and, if not, to list each other requirement for which the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date.

NERC confirms that the requirements identified by FERC are the only requirements annotated as "existing" in Table 2 of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. Recall that Table 2 assumes the Registered Entity has undergone at least one iteration of the Critical Asset identification process as required by CIP-002.

g. At page 1, under the heading "Implementation Schedule," the Version 2 Implementation Plan lists three categories. Category 2 refers to "An existing Cyber Asset becomes subject to CIP Reliability Standards, *not due to planned change*," while Category 3 refers to "A new or existing Cyber Asset becomes subject to CIP Reliability Standards *due to planned change*" (emphasis in original). We direct NERC to clarify, for purposes of these categories, the meaning of the statement "Cyber Asset becomes subject to CIP Standards." We note that pursuant to CIP-002-2 Requirement R3, a Responsible Entity must consider which of its Cyber Assets are Critical Cyber Assets essential to the operation of a Critical Asset. In that sense, all of a Responsible Entity's Cyber Assets become subject to CIP Reliability Standards when the entity undertakes to comply with CIP-002-2 Requirement R3. We also observe that at page 2, the Version 2 Implementation Plan states that the term "Cyber Asset becomes subject to the CIP standards" applies to "all Critical Cyber Assets, as well as to other (non-critical) Cyber Assets within an Electronic Security Perimeter." However, this statement does not make clear whether NERC intends that formula to be the definition of the term. We direct NERC to clarify the meaning of the term "planned change" that appears in the description of both categories, because the Version 2 Implementation Plan does not define that term.

NERC understands FERC's directive with respect to the application of CIP-002 for all Cyber Assets and clarifies that the term "Cyber Asset becomes subject to CIP standards" in the revised plan should be modified to read: "Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009." This language applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

NERC also clarifies in the Implementation Milestone Categories section of the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities that a "planned change" refers to any changes of the electric system or Cyber Assets that were planned and implemented by the Registered Entity. This contrasts with an unplanned change to the electric system that occurs through the actions of others apart from the Registered Entity. The unplanned change causes the reclassification of a Cyber Asset previously designated not to be a Critical Cyber Asset as a Critical Cyber Asset during the annual application of the CIP-002 process.

h. At page 3, the Version 2 Implementation Plan states that Category 2 applies "only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement" (emphasis in original). We direct NERC to clarify this statement because of our concern that it provides an unintended incentive for Responsible Entities to delay identification of assets that trigger the implementation timelines set forth in Table 2. For example, in January 2010 a Responsible Entity could obtain information indicating that an asset already in service should be identified as a Critical Cyber Asset. However, if the Responsible Entity does not so "identify" the asset until December 2010, the period the Version 2 Implementation Plan allows for becoming compliant would begin as much as 11 months later than if the Responsible Entity identified the asset as a Critical Cyber Asset immediately after obtaining information indicating that the asset should be so identified. We note that CIP-002-2 Requirement R3 states that a Responsible Entity shall review its list of Critical Cyber Assets "at least annually, and update it as necessary."

NERC would expect an entity to review its Critical Cyber Assets list "at least annually, and update it as necessary." In the course of a compliance audit, ERO auditors would expect to see evidence demonstrating both (1) that the audited entity had reevaluated its Critical Cyber Assets list each year during the audit period, and (2) that the audited entity incorporated newly identified Critical Cyber Assets into the list during appropriate times between such reviews. In all cases, regardless of the compliance monitoring method, NERC and Regional Entity staff will review whether an entity complied with the re-evaluation element of CIP-002-2, Requirement R3 whenever they identified a Critical Cyber Asset that was not previously on the list of Critical Cyber Assets. Note that if an in-service Critical Cyber Asset is modified or a Cyber Asset is added through construction, upgrade, or replacement by the Responsible Entity, the category "Compliant upon Commissioning" would apply. Therefore, the issue focuses on the identification of other Cyber Assets caused by an unplanned change.

i. Also at page 3, with respect to a business merger where all parties have identified Critical Cyber Assets and have "existing but different" CIP compliance plans in place, the Version 2 Implementation Plan provides that the merged Responsible Entity has one calendar year from the merger's effective date to determine either to combine the programs or operate them separately under a common Senior Manager. The Version 2 Implementation Plan further states that at the conclusion of the calendar year, the merged Responsible Entity will use the Category 2 milestones to consolidate the separate programs. We direct NERC to specify the minimum extent of difference between the compliance plans that would trigger this provision of the Version 2 plan, because, absent this specificity, any difference between the compliance plans could activate this provision. We further direct NERC to explain whether this provision would extend the time period for compliance with applicable Version 2 requirements for the merged Responsible Entity if it (a) did not identify any additional Critical Cyber Assets after the effective date of the merger; or (b) did identify such additional assets.

NERC explains its discourse in Scenario 3 of the revised plan, that any difference, including a simple difference such as the use of different anti-virus software between the two Registered Entities would trigger the provision. With respect to FERC's question pertaining to the extension of time for compliance with the standards following the one-year analysis period, NERC notes that the compliance programs would be expected to continue for any previously identified Critical Cyber Assets until the combined plan is fully implemented; any newly identified Critical Cyber Assets would be subject to the compliance schedule in Table 2 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities starting on the date of their identification. Thus, the entity remains subject to compliance with CIP standards during the transition period. Both of these provisions will be subject to review in a CIP Spot Check or Audit

j. At the last paragraph of page 4, the Version 2 plan states, "Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards." The Commission observes that the third sentence is not accurate if the phrase "these standards" is interpreted to include CIP-002-2. We direct NERC to revise this sentence to clarify its meaning.

NERC has revised the referenced language to specify that "[o]nly upon designation of

Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009."

k. We direct NERC to clarify whether the abbreviations used in Table 3 of the Version 2 Implementation Plan (BW, SC, C and AC) have the same meaning as the counterpart abbreviations in the Version 1 plan.

NERC has revised the Table 3 classifications in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for newly registered entities after April, 2008 to only include a "Compliant date" to be consistent with the term used elsewhere in the plan, NERC recognizes the continued relevance of the Compliant and Auditably Compliant designations until the retirement of the Version 1 implementation plan as discussed in item (c). However, when the Version 1 implementation plan dates are retired (*i.e.* on December 31, 2010), the terms used in that document (BW, SC, C, and AC) will no longer be used. The Compliant dates specified in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities are consistent with those specified in Table 4 of the original Version 1 Implementation Plan.

l. We observe generally that further clarification on the treatment of mergers and acquisitions at pages 3 and 4 of the Version 2 Implementation Plan is appropriate and perhaps could be achieved with explanatory text and examples in an introductory section. The Commission believes that it would be helpful to entities and promote uniform understanding if introductory explanations and/or diagrams were to address the following merger-specific instances: (1) a merger of two or more entities where none have identified a Critical Cyber Asset; (2) a merger of two or more entities where one has identified at least one Critical Cyber Asset; and (3) a merger of two or more entities where each has identified at least one Critical Cyber Asset.

NERC has significantly expanded the discussion in the plan to specifically address each of the scenarios described by FERC for newly Registered Entities based on mergers and acquisitions.

m. We also observe that one or more existing Responsible Entities that have identified at least one Critical Cyber Asset could form a new entity that heretofore has not been registered on the NERC Compliance Registry. Upon the new entity's registration, it could be argued that Table 3 of the Version 2 Implementation Plan would apply to it because it would be an entity "registering in 2008 and thereafter." Interpreted literally, Table 3 then would exempt the newly registered entity from compliance with CIP-003-2 Requirement R2 for 12 months after registration and with the remainder of the requirements of the Version 2 CIP Reliability Standards for 24 months after registration. We direct NERC to explain how it would address this situation in the context of Version 2 implementation. More broadly, because innumerable permutations of merger and acquisition scenarios exist, we direct NERC to incorporate into the Version 2 Implementation Plan explicit language to preclude unfair delay of compliance due to the structure of particular transactions.

NERC specifically addresses the situation noted in FERC's directive by noting in the introduction that the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies. More specifically, in Scenario 2, the merged Registered Entity will implement the CIP compliance implementation program of the predecessor Registered Entity with an identified Critical Cyber Asset, which will be expected to apply to any Critical Cyber Assets identified after the date of the merger. In this regard, Table 2 will apply, not Table 3 that deals with newly Registered Entities registered in April 2008 or thereafter. Similarly, under Scenario 3 that deals with predecessor Registered Entities where each has identified at least one or more Critical Cyber Asset, the language in sub-section (a) indicates that any new Critical Cyber Assets identified as a result of a merged Critical Asset identification methodology will be treated as a newly identified Critical Cyber Assets and fall under Table 2 as a result. Until such time that the methodologies are combined, the predecessor programs and methodologies will be applied, and any newly identified Critical Cyber Assets will be treated under Table 2 as well.

In summary, if an entity falls within scenarios 2 and 3 of the merger and acquisitions section that assumes a predecessor Registered Entity has previously identified at least one

Critical Cyber Asset, the existing CIP compliance implementation program(s) will carry forward to the merged Registered Entity until such time a decision is made to combine the programs. Whether or not a decision to combine the programs is made, the outcome is the same: Table 2 will apply and any newly identified Critical Cyber Assets will be implemented according to the milestones therein. Table 3 only applies to newly Registered Entities that have not previously applied the CIP-002 Critical Asset identification methodology.

C. Updated Timeline for Addressing Order No. 706 Directives

Version 2 CIP Order, P 43-44:

> 43. In Order No. 706, we directed NERC to develop a timetable as well as submit a work plan for developing and filing for approval the modifications directed by the Commission to the CIP Reliability Standards.[] While we do not object to NERC's multi-phased approach, NERC should provide more information regarding the status of these modifications, such as the inclusion of lessons learned,[] the clarification that Responsible Entities cannot except themselves from the CIP Reliability Standards,[] and identification of the core training elements and parameters for exceptional circumstances.[]
>
> 44. We direct NERC to submit as part of the compliance filing required by this order an update of the timetable that reflects the plan to address remaining Commission directives from Order No. 706. The filing should be a report of current status, addressing all of the projects including those that are underway and already planned as well as those that have been deferred or not yet scheduled, with a summary description of which Order No. 706 directives NERC plans to address during each phase.

NERC Response:

NERC has developed an approach to addressing the directives in Order No. 706 that reflects the importance of expeditiously improving the quality of the currently effective Version 1 CIP standards, and significantly increasing the emphasis of critical infrastructure protection of the bulk power system in general. Principally, these efforts resulted in the establishment of a NERC Critical Infrastructure Protection program in 2008. The primary purpose of this program is to coordinate all of NERC's efforts to improve physical and cyber security for the bulk power system of North America, as it relates to reliability. These efforts include standards

development, compliance enforcement, assessments of risk and preparedness, disseminating critical information via alerts to industry, and raising awareness of key issues.

Additionally, the program is home to the Electricity Sector Information Sharing and Analysis Center (or ES-ISAC) which monitors the bulk power system to provide real-time situation awareness leadership and coordination services to the electric industry. In addition, NERC's Critical Infrastructure Protection Committee ("CIPC") supports and provides technical subject matter expertise to both programs. The CIPC Executive Committee, along with the President and CEO of NERC, serve as the Electricity Sector Coordinating Council to collaborate with the U.S. Department of Energy ("DOE") and U.S. Department of Homeland Security ("DHS") on critical infrastructure and security matters. The DOE designated NERC as the electricity sector coordinator for critical infrastructure protection. NERC serves as the Information Sharing and Analysis Center for the electricity sector. NERC also works closely with the DHS and Public Safety Canada to ensure the critical infrastructure protection functions are coordinated with the governments of the United States and Canada.

NERC's increased focus on critical infrastructure protection has manifested itself in a number of important activities, not the least of which is oversight and improvement to the set of FERC-approved Version 1 CIP Reliability Standards as directed in Order No. 706. The timeline for implementing the directives in Order No. 706 is discussed later in this section. Since the formal establishment of the NERC CIP program in July 2008, NERC has:

- Hired a Vice President and Chief Security Officer;
- Developed and delivered compliance auditor training for the Version 1 CIP Reliability Standards;
- Developed and filed for FERC approval the Technical Feasibility Exception process for Version 1 and future CIP Reliability Standards;
- Conducted a High Impact Low Frequency Workshop to engage industry and U.S. government leaders on appropriate actions to consider in addressing this threat;

- Conducted a primary and supplemental survey of entities under compliance with CIP-002-1 to determine how Registered Entities are applying methodologies to identify Critical Cyber Assets;
- Coordinated with the CIPC to develop guidance documents to support Critical Asset identification per CIP-002-1, Critical Cyber Asset identification that is currently in process;
- Issued six advisories in 2009 that directly address Cyber Assets (a subset of CIP), issued three advisories in 2009 that address CIP in general (H1N1 advisories), and issued three Recommendations addressing cyber assets in 2008;
- Continues to support through active participation and through comment opportunities the advancement and integration of SmartGrid equipment on the grid;
- Proposed two updated versions of CIP Reliability Standards based on directives issued in Order No. 706 and in the Version 2 CIP Order, while pursuing more substantive changes to the CIP reliability standards based on the remaining Order No. 706 directives;
- Established the North American Synchro-Phasor Initiative;
- Filed an Implementation Plan for U.S. nuclear power plants relative to NERC's Version 1 CIP Reliability Standards;
- Coordinated with the Nuclear Regulatory Commission on the development of a memorandum of understanding regarding implementation of critical infrastructure protection at U.S. nuclear power plants; and
- Filed numerous standards interpretations to Version 1 CIP Reliability Standards.

This compendium of critical infrastructure activities demonstrates NERC's and the industry's commitment to improving critical infrastructure protection for the bulk power system and preserving reliability. At the core of these activities, however, is the establishment of a set of mandatory and enforceable Reliability Standards that Registered Entities are obligated to implement for their Cyber Assets relating to the bulk power system. NERC submitted in August, 2006 and FERC approved in January 2008 an initial set of CIP Reliability Standards, referred to as the Version 1 CIP standards. While noting that these standards serve a useful reliability purpose, they establish the minimum set of expectations and require significant improvement to achieve the level of ultimate acceptability to protect the bulk power system.

Accordingly, FERC identified a lengthy list of improvements through directives set forth in Order No. 706 for NERC to address. Some of the directives require changes to the standards themselves, requiring industry stakeholders to develop and approve these changes through the *Reliability Standards Development Procedure*. Other directives regarding guidance in implementing the existing CIP standards were assigned to NERC's Critical Infrastructure Protection Committee to develop or are awaiting further refinement to the requirements before developing the needed guidance. For directives requiring standards changes, NERC, working through its industry drafting team and the Standards Committee, elected to apportion these improvements in a multi-phase approach. Each phase would result in a separate filing to FERC, representing a new version of the standards. The first phase of this improvement project that resulted in the Version 2 CIP standards addressed the following items that were of significance to FERC in its Order No. 706 and other non-controversial items the team believed would receive industry acceptance:

- removal of the term "reasonable business judgment" from the purpose section of each Reliability Standard;
- removal of the term "acceptance of risk" from each Reliability Standard;
- specification in CIP-002-2 Requirement R4 that the senior manager must annually approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets;
- requirement in the CIP-003-2 Applicability section that all Responsible Entities must comply with CIP-003-2 Requirement R2;
- specification in CIP-003-2 Requirement R2 that a single manager with overall responsibility and authority must be designated;
- specification in CIP-003-2 Requirement R2.3 that delegations of authority must be documented;
- specification in CIP-004-2 Requirement R2 that all employees with authorized access must be trained prior to access, except in specified circumstances;

- clarification in CIP-004-2 Requirement R3 that the Responsible Entity shall have a documented personnel risk assessment program, prior to personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets;
- clarification in CIP-006-2 Requirement R1 that the Responsible Entity shall document, implement and maintain a physical security plan, approved by the senior manager; and
- identification of a Responsible Entity's compliance schedule in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

NERC filed a request for approval of these standards on May 22, 2009 and FERC approved them in its Version 2 CIP Order. Additional revisions to the Version 2 standards directed by FERC in its Version 2 CIP Order are presented as Version 3 CIP standards in this filing. In order to meet the ninety-day delivery timeframe for the Version3 CIP standards, the NERC drafting team received approval from the Standards Committee to use a modified development process that slightly differs from that customarily used and currently approved in NERC's Rules of Procedure, Appendix 3A.

NERC has outlined an updated plan in **Exhibit 5** to this filing to address the remaining directives originating from Order No. 706. For completeness, **Exhibit 5** includes all directives from the Order. For each item in the list, NERC includes a description of its current status and the version of the development activity in which the item has been or will be addressed. NERC intends to address the remaining activities in future submissions to FERC.

NERC also acknowledges various items that NERC was directed to *consider* in Order No. 706. To the extent the issues for consideration are appropriate for consideration during the Version 4 activities described below (*i.e.*, activities specifically focused on FERC's directives in Order No. 706), the team will consider the items. Otherwise, the team will consider the items in future development activities.

In order to improve consistency in identifying Critical Cyber Assets based on the experiences in applying the current CIP-002-1 standard requirements, NERC will first propose a

revised CIP-002 standard that includes a significant paradigm shift in the approach relative to the current mandatory expectations. This change in approach was conceptually outlined in the drafting team's concept paper, *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions* that was presented for industry review and comment in July 2009. The proposed methodology proposes a mapping of Bulk Electric System ("BES") subsystems into categories based on their impact on the reliability or operability of the BES. The drafting team posted the first draft of CIP-002-4 for an informal industry comment period on December 29, 2009. Using the NERC Standards Development Process, this Version 4 activity and delivery of a revised CIP-002-4 standard is expected to be completed in May 2010. NERC will advise FERC if there should be a significant change in this schedule.

The next significant portion of work, noted as the second part of Version 4, is the development of a suite of security requirements (controls) for each of the impact categories identified in CIP-002-4 for each BES subsystem, identified as generation, transmission, and control centers. These requirements are intended to modify, replace, retire, and in some cases, add to the current CIP-003 through CIP-009 standard requirements. The body of work associated with the second part of Version 4 represents the most significant volume of work remaining and includes many of the Order No. 706 directives not yet addressed. NERC's current plan is to file the updated versions of CIP-003 through CIP-009 by year-end 2010.

The remaining activities, identified as post Version 4, represent the subset of directives and considerations from Order No. 706 that NERC believes will require significantly more time to discuss and develop the appropriate technical solutions. NERC will begin working on these post-Version 4 modifications once the Version 4 standards are filed with FERC. At that time, a schedule for those activities will be developed. The key post-Version 4 activities are:

- defense in depth approaches for electronic and physical security perimeter (Order No. 706, PP 496, 502, 503, 572, 575);
- vulnerability assessments (Order No. 706, PP 547, 643) and operational exercises for recovery (Order No. 706, P 725); and,
- forensics (Order No. 706, PP 706, 710).

While NERC understands the obligation to address these directives, NERC also believes there needs to be a more thoughtful and deliberate technical discussion on the approach used to address these items due to the potential detrimental impacts to reliability or extraordinary costs to implementation that could result with a literal implementation of the directives. NERC believes it prudent to engage FERC staff and industry technical experts to develop an approach to these directives that achieve the intended outcome — to protect and preserve the reliability of the Bulk Power System — while not introducing adverse reliability outcomes or exorbitant costs to implement.

NERC notes that the concepts contained in these directives are complex, and will require extensive debate, discussion, research, and in at least one case, vendor research and development before a set of mandatory and enforceable requirements can be drafted that will allow compliance by all applicable entities on all applicable systems. NERC does not believe that this can be accomplished in the timeframe proposed for the Version 4 changes. NERC also notes that there will be significant departure from the current standards methodology of protecting Critical Cyber Assets, moving to an approach where all BES Cyber Systems are protected, which is a significant increase in the scope of applicability for the CIP standards. Given this increase in current scope, NERC does not believe that these four areas can be properly addressed in the proposed timeframe for Version 4.

With respect to the defense in depth approaches for electronic and physical security perimeters, NERC notes that there is need for extensive debate and discussion within the

industry on exactly how to accomplish the directives noted in Order No. 706. If taken literally, the defense in depth principle would seem to require two independent methods of either physical or electronic security surrounding a protected asset (even though the Order indicates that this literal interpretation is not intended). While this is practical and achievable in a control center or data center environment, it is problematic in substation or generating plant environments. As discussed in NERC's filing in response to the NOPR,[10] there are also safety and performance issues related to multiple layers of defense in depth.

FERC also notes that entities may wish to rely on Technical Feasibility Exceptions when claiming that multiple layers of defense in depth are not practical. However in its development of future versions of the CIP standards, the drafting team is attempting to reduce the necessity and reliance on technical feasibility exceptions, based on input from NERC, the Regional Entities, and the industry. Careful wording of the requirements is therefore necessary in order to reduce continued reliance on Technical Feasibility Exceptions, thereby streamlining the audit process, and more directly communicating mandatory and enforceable requirements to the stakeholders.

With respect to vulnerability assessments and operational exercises for recovery, NERC notes that the performance of vulnerability assessments on live operations is challenging, and if done improperly, can be detrimental to the reliable operation of the systems, and therefore detrimental to reliable operation of the bulk power system.[11] NERC acknowledges that a vulnerability assessment should be performed against the systems employed in the bulk power system, but entities must work closely with their technology providers to develop safe test procedures for assessments on *live* systems or develop approaches to perform testing in a test

[10] *See* NERC's October 5, 2007 filing in response to Notice of Proposed Rulemaking ("NERC's Filing in Response to NOPR"), Section J.
[11] *See* NERC's Filing in Response to NOPR, Section K.

environment that closely replicates the live system. In many cases, particularly with legacy systems or for custom built systems of which there is only a single copy, full test environments cannot be made available for performing vulnerability tests or recovery exercises. In these cases, it is possible that hardware and software are no longer manufactured, and cannot be purchased for such purpose, and the redundant systems deployed for availability of critical functions (*e.g.*, a primary-reserve control system) cannot be sufficiently decoupled to allow full vulnerability testing or recovery exercises of the system without impacting the live system.

NERC is working with entities on a voluntary basis to further explore how to best design and develop cyber focused operational exercises for system recovery. NERC's Critical Infrastructure Protection program has engaged both registered entities and government stakeholders to conduct a series of table top exercises, such as Secure Grid 2009 and several Cyber Risk Preparedness Assessments, to advance the development of recovery exercises that are driven by cyber induced outages. The work to date has demonstrated the value of developing cyber scenarios to drive recovery exercises. NERC will continue to work with stakeholders to provide guidance and examples for the development of cyber-based recovery exercises.

NERC also believes that some aspects of the directives are better suited to be included in guidance documents, which can be developed once the revised requirements are complete.

With respect to forensics, NERC notes that the term "forensics" connotes specific methods of handling data as evidence, including "chain of custody" and protection of data during analysis.[12] NERC believes that data analysis associated with failures and misuse of systems is important, but is not currently feasible for a large portion of the installed technology that is important to the operation of the bulk power system. Many field devices (*e.g.*, relays in use at

[12] *See* NERC's Filing in Response to NOPR, Section L

transmission substations) do not currently have rapid data extraction techniques available or, in many cases, sufficient security logging, that facilitate the extraction of operational and investigative data in the field while continuing to operate. Research and development by equipment vendors will be needed in order to produce equipment that is capable of rapid unobtrusive data extraction. NERC is involved in both the DHS Control Systems Security Program and the DOE National Supervisory Control and Data Acquisition ("SCADA") Test Bed to support continued advancement of security response and forensics capabilities and tools for electric infrastructure systems. At the point where sufficient advancements are made, the developed equipment will need to be purchased and installed in the field before specific data extraction requirements can be made mandatory and enforceable.[13]

Finally, NERC points out that because of the paradigm shift in the approach for its critical infrastructure protection standards to provide protection for all BES cyber systems, beginning with CIP-002-4, several of the directives and considerations in Order No. 706 are rendered meaningless. Therefore, FERC's concerns will have been ameliorated by virtue of the shift in philosophical approach to categorizing cyber systems based on the BES subsystem impact mapping.

V. CONCLUSION

The North American Electric Reliability Corporation respectfully requests that FERC accept this filing and Attachments in compliance with Paragraphs 30, 38, 40, 41, 43, and 44, of the Version 2 CIP Order. As part of this filing, NERC requests that FERC approve as set out in **Exhibits 1, 4a, 4b, 6a, and 6b** of the filing:

- Version 3 CIP Standards and associated changes to VRFs and VSLs;

[13] *See* also the previous discussion on decreasing reliance on technical feasibility exceptions.

- Revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to become effective on April 1, 2010;
- Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3; and
- Carrying forward Version 2 VRFs and VSLs for un-modified requirements from Version 2.

in accordance with Section 215(d)(1) of the FPA and Part 39.5 of FERC regulations.

Respectfully submitted,

/s/ Holly A. Hawkins

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

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

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 29th day of December, 2009.

/s/ Holly A. Hawkins
Holly A. Hawkins

Attorney for North American Electric Reliability Corporation

EXHIBIT 1

CIP Version 3 Reliability Standards Proposed for Approval.

A. Introduction

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

2. **Number:** CIP-006-~~2~~3

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

4. **Applicability:**

   4.1. Within the text of Standard CIP-006-~~2~~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-006-~~2~~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-~~2~~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. Requireme nts

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

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

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

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

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

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter ~~of personnel not authorized for unescorted access.~~.

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

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

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

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3 Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.

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

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

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures

specified in Requirement CIP-008-~~2.~~3. One or more of the following monitoring methods shall be used:

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

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

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

R7. Access Log Retention — The ~~responsible entity~~Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-~~2~~3 for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	

A. Introduction

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

2. Number: CIP-008-~~2~~3

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

4. Applicability

4.1. Within the text of Standard CIP-008-~~2~~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-008-~~2~~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-~~2~~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. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

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

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

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

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

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

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

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

C. Measures

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-~~2~~3 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

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

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~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.	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Font: 10 pt
Formatted: Left
Formatted: Left
Formatted: Font: 10 pt

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3

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

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

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

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "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-002-3:

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.

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

1.5.1 None.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Adopted by Board of Trustees	

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.

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).

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

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

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

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

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, 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.

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Adopted by Board of Trustees	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-3

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

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

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

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

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

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

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program**.** Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Adopted by Board of Trustees	

A. Introduction

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

2. Number: CIP-005-3

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 a 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.

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		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access	

		Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Adopted by Board of Trustees	

A. Introduction

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

2. Number: CIP-006-3

3. Purpose: Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 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-006-3, "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-006-3:

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

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

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

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

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

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

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

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

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

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

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

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

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

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

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

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

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	
3	12/16/09	Adopted by Board of Trustees	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

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.

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-003-3 Requirement R5 and Standard CIP-004-3 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-008-3.

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-005-3.

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

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

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

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

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

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

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

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

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 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. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Adopted by Board of Trustees	

A. Introduction

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

2. Number: CIP-008-3

3. Purpose: Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-23should 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-008-3, "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-008-3:

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

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

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

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

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

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

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

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

C. Measures

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-3 for the previous full calendar year unless directed by its Compliance Enforcement

Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

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

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

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

2. Number: CIP-009-3

3. Purpose: Standard CIP-009-3 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-3 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-009-3, "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-009-3:

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Adopted by Board of Trustees	

EXHIBIT 2

Record of Development of Proposed Reliability Standards.

Project 2009-21
Cyber Security Ninety-Day Response

Status:
The recirculation ballot window for critical infrastructure protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3, a general implementation plan, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* ended December 14, 2009. The ballot pool approved the standards and implementation plans, which will be submitted to the NERC Board of Trustees for approval.

Purpose / Industry Need:
To modify certain Critical Infrastructure Protection (CIP) Reliability Standards in response to the directives issued in the Federal Energy Regulatory Commission's (FERC) September 30, 2009 Order Approving Revised Reliability Standards For Critical Infrastructure Protection And Requesting Compliance Filing: http://www.nerc.com/files/OrderApproving_V2_CIP-002_CIP-009-09302009.pdf

Draft	Action	Dates	Results	Consideration of Comments
Version 3 Cyber Security Standards (excluding CIP-006-3) Clean **(18)** Redline to Last Approval **(19)** CIP-006-3 Clean **(20)** Redline to Last Approval **(21)** Redline to Last Posting **(22)** Version 3 Implementation Plan Clean **(23)** Redline to Last Approval **(24)** Redline to Last Posting **(25)** Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities Clean **(26)** Redline to Last Approval **(27)** Redline to Last Posting **(28)** CIP Version 3 Violation Risk Factors Clean **(29)** Redline to Last Approval **(30)** CIP Version 3 Violation Severity Levels Clean **(31)** Redline to Last Approval **(32)**	Recirculation Ballot Vote>> | Info>> **(36)**	12/03/09 - 12/14/09	Summary>> **(37)** Full Record>> **(38)**	
	Initial Ballot Vote>> | Info>> **(17)**	11/20/09 - 11/30/09 (closed)	Summary>> **(33)** Full Record>> **(34)**	Consideration of Comments>> **(35)**
Version 3 Cyber Security	Pre-ballot Review	10/27/09 -		

Standards Clean **(1-1g)** Redline to last posting **(2-2g)** (zip files) SAR **(3)** CIP Version 3 Violation Risk Factors Clean **(4)** Redline **(5)** CIP Version 3 Violation Severity Levels Clean **(6)** Redline **(7)** Version 3 Implementation Plan Clean **(8)** Redline to last posting **(9)** Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities Clean **(10)** Redline to last posting **(11)** **Supporting Materials:** Comment Form (Word) **(12)**	Join>> | Info>>**(16)**	11/20/09 (closed)		
	Comment Period Submit Comments>> Info>> **(13)**	10/13/09 - 11/12/09 (closed)	Comments Received>> **(14)**	Consideration of Comments>> **(15)**

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3

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

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

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

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "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-002-3:

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.

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

1.5.1 None.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	

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.

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).

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

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

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

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

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, 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.

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-3

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

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

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

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

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

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

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program**.** Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	

A. Introduction

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

2. Number: CIP-005-3

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 a 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.

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		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity.	

		Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	

A. Introduction

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

2. Number: CIP-006-3a

3. Purpose: Standard CIP-006-3a is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3a 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-006-3a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-006-3a:

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

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

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

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

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

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components:

R1.6.1. Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.

R1.6.2. Requirement for continuous escorted access within the Physical Security Perimeter of visitors.

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

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

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

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

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

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

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

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

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

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

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3a for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3a		Updated version numbers from -2 to -3a Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	

Appendix 1

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

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

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

CIP-006-1 – Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

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

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

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.

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-003-3 Requirement R5 and Standard CIP-004-3 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-008-3.

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-005-3.

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

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

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

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

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

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

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

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

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 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. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	

A. Introduction

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

2. Number: CIP-008-3

3. Purpose: Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-23should 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-008-3, "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-008-3:

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

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

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

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

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

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

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

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

C. Measures

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-3 for the previous full calendar year unless directed by its Compliance Enforcement

Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

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

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

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

2. Number: CIP-009-3

3. Purpose: Standard CIP-009-3 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-3 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-009-3, "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-009-3:

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~2~~3

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

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

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

Standard CIP-002-~~2~~3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-~~2~~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-002-~~2~~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.

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-~~2~~3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-~~2~~3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

1.5.1 None.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Updated version number from -2 to -3	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Font: Verdana, 10 pt
Formatted: Font: Verdana, 10 pt
Formatted: Font: Verdana, 10 pt
Formatted: Left
Formatted: Font: Verdana, 10 pt

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~2~~3

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

4. **Applicability:**

   4.1. Within the text of Standard CIP-003-~~2~~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-~~2~~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-~~2~~3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-~~2~~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-~~2~~3 through CIP-009-~~2~~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.

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

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-~~2~~3 through CIP-009-~~2~~.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-~~2~~3 through CIP-009-~~2~~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).

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

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

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

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

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-~~2~~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.

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Update version number from -2 to -	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Font: 10 pt
Formatted: Left

		3	

A. Introduction

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

2. **Number:** CIP-004-~~2~~3

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

4. **Applicability:**

   4.1. Within the text of Standard CIP-004-~~2~~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-004-~~2~~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-~~2~~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. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

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

Formatted: French (France)

Formatted: French (France)

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

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

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

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-~~2~~3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-~~2~~3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program**.** Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Update version number from -2 to -3	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Table Col Heading
Formatted: Font: Times New Roman, Not Bold
Formatted: Font: Times New Roman
Formatted: Table Col Heading, Left
Formatted: Font: 10 pt

Formatted: Bottom: 0.5"

A. Introduction

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

2. Number: CIP-005-~~2~~3

3. Purpose: Standard CIP-005-~~2~~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-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. Applicability

4.1. Within the text of Standard CIP-005-~~2~~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-~~2~~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-~~2~~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-~~2~~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 a specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3 Requirement R3; Standard CIP-007-~~2~~3 Requirements R1 and R3 through R9; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~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-~~2~~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.

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

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

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

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

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

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

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

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

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

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-~~2~~3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-~~2~~3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-~~2~~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-~~2~~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-~~2~~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-~~2~~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		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.	

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Left

		Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Update version from -2 to -3	~~Revised~~

Formatted: Font: Times New Roman, Not Bold

Formatted: Table Col Heading

Formatted: Font: Times New Roman, Not Bold

Formatted: Table Col Heading, Left

Formatted: Font: 10 pt, Not Bold

A. Introduction

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

2. **Number:** CIP-006-~~2~~3a

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

4. **Applicability:**

   4.1. Within the text of Standard CIP-006-~~2~~3a, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-006-~~2~~3a:

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

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-~~2~~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. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

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

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

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

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

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~3 Requirement R4.

R1.6. ~~Continuous~~A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components:

R1.6.1. Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.

R1.6.2. Requirement for continuous escorted access within the Physical Security Perimeter of ~~personnel not authorized for unescorted access.~~visitors.

Formatted

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

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

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

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3a Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.

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

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

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-~~2.~~3. One or more of the following monitoring methods shall be used:

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

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

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

R7. Access Log Retention — The ~~responsible entity~~Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-~~2~~3a for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
~~2~~3a	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Updated version numbers from -2 to -3a Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Font: Times New Roman, Not Bold
Formatted: Font: Times New Roman, Not Bold
Formatted: Table Col Heading
Formatted: Table Col Heading, Left
Formatted: Font: 10 pt

Appendix 1

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

> **R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> **R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.**

CIP-006-1 – Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

> **1.4. Additional Compliance Information**
>
> **1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.**

Formatted: Bottom: 0.5"

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~2~~3

3. Purpose: Standard CIP-007-~~2~~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-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. Applicability:

4.1. Within the text of Standard CIP-007-~~2~~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-~~2~~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-~~2~~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-~~2~~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-~~2~~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-~~2~~3 Requirement R5.

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

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-~~2~~3 Requirement R5 and Standard CIP-004-~~2~~3 Requirement R4.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-~~2~~3.

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

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

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

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

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

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

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

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

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-~~2~~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-~~2~~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	

Formatted: Left

Formatted Table

		Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Updated version numbers from -2 to -3	~~Revised~~

Formatted: Font: 10 pt

Formatted: Left

Formatted: Font: 10 pt

Formatted: Left

Formatted: Font: 10 pt

A. Introduction

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

2. **Number:** CIP-008-~~2~~3

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

4. **Applicability**

   4.1. Within the text of Standard CIP-008-~~2~~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-008-~~2~~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-~~2~~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. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

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

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

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

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

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

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

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

C. Measures

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-~~2~~3 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

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

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~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.	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Font: 10 pt
Formatted: Left
Formatted: Left
Formatted: Font: 10 pt

Formatted: Bottom: 0.5"

A. Introduction

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

2. **Number:** CIP-009-~~2~~3

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

4. **Applicability:**

   4.1. Within the text of Standard CIP-009-~~2~~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-009-~~2~~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-~~2~~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. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

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

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

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

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

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

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

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-~~2~~3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Updated version numbers from -2 to -3	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Font: 10 pt
Formatted: Left
Formatted: Left
Formatted: Font: 10 pt

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title of Proposed Standard:	Cyber Security Ninety-day Response
Request Date:	October 2, 2009
SC Approval Date:	October 7, 2009

SAR Requester Information		**SAR Type** (*Check a box for each one that applies.*)	
Name:	NERC Staff	☐	New Standard
Primary Contact:	David Taylor	X	Revision to existing Standards
Telephone: **Fax:**	(609)651-5089	☐	Withdrawal of existing Standard
E-mail:	David.Taylor@NERC.net	☐	Urgent Action

Purpose:

To modify certain Critical Infrastructure Protection (CIP) Reliability Standards and associated Implementation Plan in respond to the directives issued in the Federal Energy Regulatory Commission's (FERC) September 30, 2009 Order Approving Revised Reliability Standards For Critical Infrastructure Protection And Requesting Compliance Filing.

Industry Need:

On May 22, 2009, NERC in its capacity as the Electric Reliability Organization (ERO) filed eight revised CIP Reliability Standards for approval with the Commission, to protect the Bulk-Power System from malicious or unintentional cyber events. They require Bulk-Power System users, owners, and operators to establish a risk-based assessment methodology to identify critical assets and the associated critical cyber assets essential to the critical assets' operation. Once the critical cyber assets are identified, the CIP Reliability Standards require, among other things, that the Responsible Entities establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. The eight Reliability Standards are as follows:

CIP-002-2 – Cyber Security – Critical Cyber Asset Identification: Requires a Responsible Entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

CIP-003-2 – Cyber Security – Security Management Controls: Requires a Responsible Entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1.

CIP-004-2 – Cyber Security – Personnel and Training: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.

CIP-005-2 – Cyber Security – Electronic Security Perimeter(s): Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002-1.

CIP-006-2 – Cyber Security – Physical Security: Requires a Responsible Entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

CIP-007-2 – Cyber Security – Systems Security Management: Requires a Responsible Entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

CIP-008-2 – Cyber Security – Incident Reporting and Response Planning: Requires a Responsible Entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

CIP-009-2 – Cyber Security – Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

On September 30, 2009 the Commission approved Version 2 of the CIP Reliability Standards with an effective date of April 1, 2010. In its September 30, 2009 Order the Commission directed NERC to make additional changes to two of the Standards (CIP-006-2 and CIP-008-2) and the associated Implementation Plan. The Order directed NERC to file the modified standards and Implementation Plan within 90 days.

The modifications to the NERC set of reliability standards and associated Implementation Plan requested in this SAR will enable NERC to comply with the FERC directives issued on September 30, 2009 and will ensure the protection of the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operation of the North American bulk power system.

Brief Description:

The Commission's September 30, 2009 Order directs NERC to submit a compliance filing within 90 days of the Order (i.e., by December 28, 2009) which, among other things, includes the following modifications:

- A modification to Reliability Standard CIP-006-2 – Cyber Security — Physical Security to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit.
- A modification to Reliability Standard CIP-008-2 – Cyber Security — Incident Reporting and Response Planning, Requirement R1.6 to remove the last sentence of CIP-008-2 Requirement R1.6.
- A revised Version 2 Implementation Plan addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to the September 30 Order.

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

The documents recommended to be modified and the associated specific modifications are attached. Please refer to the attached documents for the detailed changes.

Although the Commission directed changes to only two of the eight CIP-002-2 thru CIP-009-2 reliability standards, conforming changes are proposed for the remaining six CIP Reliability Standards (CIP-002-2 thru CIP-005-2, CIP-007-2, CIP-009-2) to correct the cross references within the set of standards. If left untouched, the Purpose statements, and many requirements within the set of standards would be incorrect as they all reference CIP-002-2 through CIP-009-2.

Reliability Functions

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

Reliability and Market Interface Principles

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

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

Related Standards

Standard No.	Explanation
CIP–002–2	Cyber Security — Critical Cyber Asset Identification – Conforming changes
CIP–003–2	Cyber Security — Security Management Controls – Conforming changes
CIP–004–2	Cyber Security — Personnel and Training – Conforming changes
CIP–005–2	Cyber Security — Electronic Security Perimeter(s) – Conforming changes
CIP-006-2	Cyber Security — Physical Security – FERC directed modifications
CIP–007–2	Cyber Security — Systems Security Management – Conforming changes
CIP–008–2	Cyber Security — Incident Reporting and Response Planning – FERC directed modifications
CIP–009–2	Cyber Security — Recovery Plans for Critical Cyber Assets – Conforming changes

Related SARs

SAR ID	Explanation

Regional Variances

Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition fromCIP-002-2 through CIP-009-2 to CIP-002-3 through CIP-009-3.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 3 CIP-002-3 thru CIP-009-32 Standards:

Index:

Standard Number CIP-003 — Security Management Controls			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP–003–3	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.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	MEDIUM
CIP–006-3a	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components:	MEDIUM
CIP–006-3a	R1.6.1	Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.	MEDIUM
CIP–006-3a	R1.6.2	Requirement for continuous escorted access within the Physical Security Perimeter of visitors.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
		with the requirements of Standard CIP-008-3.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition fromCIP-002-2 through CIP-009-2 to CIP-002-3 through CIP-009-3.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 3 CIP-002-3 thru CIP-009-32 Standards:

Index:

Standard Number CIP-003 — Security Management Controls			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP–003–~~2~~3	R2.3.	Where allowed by Standards CIP-002-3~~2~~ through CIP-009-~~2~~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.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~ 3 Requirement R4.	MEDIUM
CIP–006-3a~~CIP-006-2~~	R1.6~~R1.6.~~	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components:~~Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.~~	MEDIUM~~MEDIUM~~
CIP–006-3a	R1.6.1	Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.	MEDIUM
CIP–006-3a	R1.6.2	Requirement for continuous escorted access within the Physical Security Perimeter of visitors.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~ 3 Requirement R3; Standard CIP-005-~~2~~ 3 Requirements R2 and R3; Standard CIP-006-~~2~~ 3a Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-~~2~~3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
		least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.	

Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-2 through CIP-009-2 into CIP-002-3 through CIP-009-3.

Proposed Violation Severity Levels for the CIP Version 3 Series of Standards (Project 2009-21):

Index:

Standard Number CIP-005-3 — Electronic Security Perimeter(s)				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3, Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-33; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
R1.6. (V3 proposed)	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	The Responsible Entity did not include or implement a visitor control program in its physical security plan.
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3aRequirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	CIP-008-3; and Standard CIP-009-3.	3.	CIP-008-3; and Standard CIP-009-3.	Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
R5.	N/A	The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.	The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.	The Responsible Entity **has not documented nor implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
		• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-3.

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-3 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-003-3 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-003-3 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-003-3 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).
R5.1.3.	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-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
R7.	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-	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-005-3 **but** did not address	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-005-3 **but** did not address disposal as	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-

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	005-3 **but** did not maintain records as specified in R7.3.	redeployment as specified in R7.2.	specified in R7.1.	3.
R9.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 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-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-2 through CIP-009-2 into CIP-002-3 through CIP-009-3.

Proposed Violation Severity Levels for the CIP Version 3 Series of Standards (Project 2009-21):

Index:

Standard Number CIP-005-~~2~~ 3 — Electronic Security Perimeter(s)				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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-003-3~~2~~; Standard CIP-004-3~~2~~ Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a~~2~~ Requirements~~s~~ R3, Standard CIP-007-3~~2~~ Requirements R1 and R3 through R9;~~,~~ Standard CIP-008-3~~2~~; and Standard ~~CIP-009-2~~CIP-009-3.	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-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3;~~,~~ Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3; Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9;~~,~~ Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	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-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3; Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is ~~not~~ provided without four (4) or more of the protective measures as specified in Standard ~~CIP-003-2~~CIP-003-33; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3;~~,~~ Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3;~~,~~ Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9;~~,~~ Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with ~~CIP-004-2~~CIP-004-3 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with ~~CIP-004-2~~CIP-004-3 Requirement R4.
R1.6. (V3 proposed)~~R1.6.~~	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~N/A~~	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~N/A~~	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.~~N/A~~	The Responsible Entity did not include or implement a visitor control program in its physical security plan.~~The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.~~
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3;	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.
R5.	N/A	The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without	The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without	The Responsible Entity **has not documented nor implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with ~~CIP-008-2~~CIP-008-3.

Standard Number ~~CIP-007-2~~CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in ~~CIP-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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).
R5.1.3.	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-003-2~~CIP-003-3 Requirement R5 and Standard ~~CIP-004-2~~CIP-004-3 Requirement R4.
R7.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security	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	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	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security

Standard Number ~~CIP-007-2~~CIP-007-3 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Perimeter(s) as identified and documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not maintain records as specified in R7.3.	documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not address redeployment as specified in R7.2.	documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not address disposal as specified in R7.1.	Perimeter(s) as identified and documented in Standard ~~CIP-005-2~~CIP-005-3.
R9.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard ~~CIP-007-2~~CIP-007-3 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-007-2~~CIP-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–3 — Cyber Security — Critical Cyber Asset Identification
CIP–003–3 — Cyber Security — Security Management Controls
CIP–004–3 — Cyber Security — Personnel and Training
CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–3 — Cyber Security — Physical Security
CIP–007–3 — Cyber Security — Systems Security Management
CIP–008–3 — Cyber Security — Incident Reporting and Response Planning
CIP–009–3 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date

The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 3 of the NERC Cyber Security Standards CIP-002-3 to CIP-009-3.

Version 1 Implementation Plan Retirement

The Version 1 Implementation Plan will be retired once all Entities in Tables 1, 2, and 3 of that plan have achieved their Compliant state.

Version 2 Implementation Plan Retirement

The Version 2 Implementation Plan will be retired on April 1, 2010 or on a Version 1 legacy date for compliance that goes beyond April 1, 2010, whichever is later.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version ~~2~~3 of Cyber Security Standards CIP-002-~~2~~3 through CIP-009-~~2~~3

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

~~Modified~~Applicable Standards

The following standards ~~have been modified~~are covered by this Implementation Plan:

CIP–002–~~2~~3 — Cyber Security — Critical Cyber Asset Identification
CIP–003–~~2~~3 — Cyber Security — Security Management Controls
CIP–004–~~2~~3 — Cyber Security — Personnel and Training
CIP–005–~~2~~3 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–~~2~~3 — Cyber Security — Physical Security
CIP–007–~~2~~3 — Cyber Security — Systems Security Management
CIP–008–~~2~~3 — Cyber Security — Incident Reporting and Response Planning
CIP–009–~~2~~3 — Cyber Security — Recovery Plans for Critical Cyber Assets

~~Red-line versions of the above~~These standards are posted for ballot by NERC together with this Implementation Plan. When these ~~modified~~ standards become effective, ~~the~~all prior versions of these standards ~~and their Implementation Plan~~ are retired.

Compliance with Standards

Once these standards become effective, the ~~responsible entities~~Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

~~Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.~~

Proposed Effective Date

~~The proposed effective date for these modified standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters) after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).~~

~~For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.~~

The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 3 of the NERC Cyber Security Standards CIP-002-3 to CIP-009-3.

Version 1 Implementation Plan Retirement

The Version 1 Implementation Plan will be retired once all Entities in Tables 1, 2, and 3 of that plan have achieved their Compliant state.

Version 2 Implementation Plan Retirement

The Version 2 Implementation Plan will be retired on April 1, 2010 or on a Version 1 legacy date for compliance that goes beyond April 1, 2010, whichever is later.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of either Version 2 or Version 3 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone date in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the risk-based Critical Asset identification methodology. Upon a subsequent annual application of the risk-based Critical Asset identification method in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009, in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, and Version 3) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2', or '-3') will be applied to that particular reference.
[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the *Compliant* milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the *Compliant* milestone date has been reached.

For those NERC Reliability Standard requirements that include a prescribed records retention period (e.g., retention of logs for 90 days), a Responsible Entity is expected to begin collection and retention of the required "data," "documents," "documentation," "logs," and "records" by the *Compliant* milestone date in Table 2.

For retention requirements that are triggered by a specific event (e.g., a reportable incident), collection and retention of the required "data," "documents," "documentation," "logs," and "records" begins with the triggering event. In this instance, the requirement for records collection and retention does not begin until the *Compliant* milestone date in Table 2 is reached and only applies to triggering events occurring after the *Compliant* milestone date.

For those NERC Reliability Standard requirements that do not include a specified periodicity or records retention requirement, a Responsible Entity is expected to have available all records required to demonstrate compliance to these requirements by the *Compliant* milestone date in Table 2.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC in April 2008 or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by the Responsibility Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsibility Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must

therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on established criteria or thresholds in the Responsible Entity's existing risk-based Critical Asset identification method (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of that risk-based Critical Asset Identification process is required annually (by CIP-002 R2), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

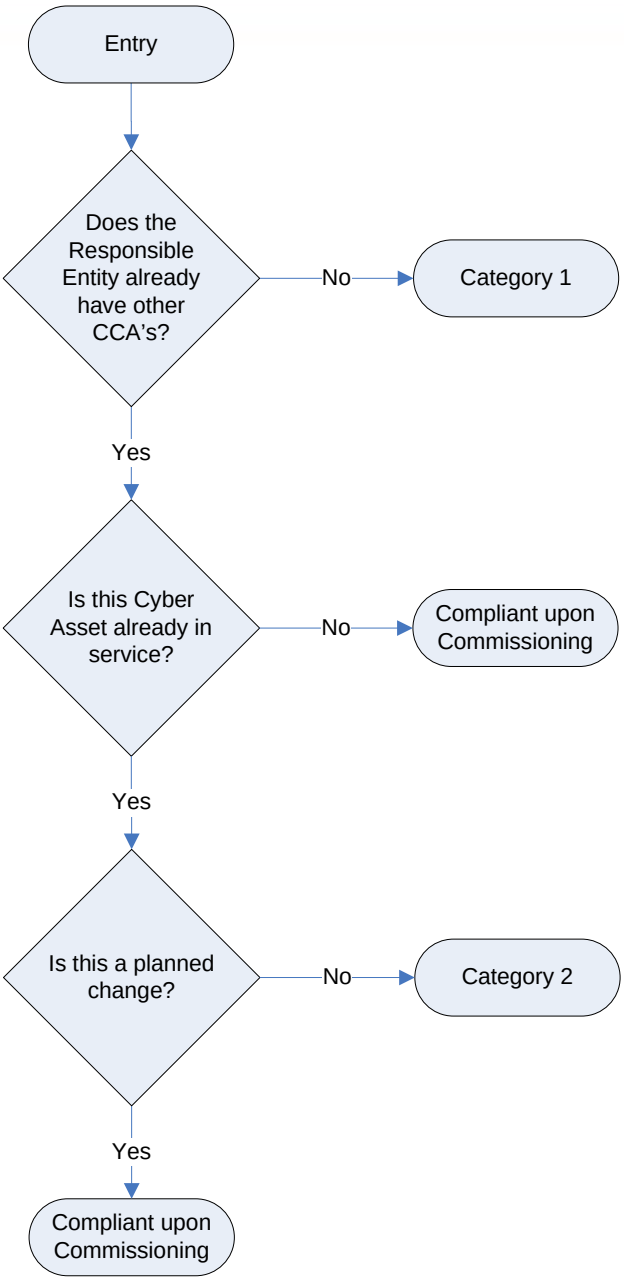


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on planning or impact studies) upon its commissioning or activation.
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset.
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset.
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies.

1. **Category 1 Scenario:**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is the NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology implementation by each predecessor Responsible Entity.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate risk-based Critical Asset identification methodology implementation while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of risk-based Critical Asset identification methodology(ies) as required in CIP-002 R2, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate methodologies, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the risk-based Critical Asset identification methodology as required in CIP-002 R2, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R3. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Category 2 Scenario:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

   Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology from Scenario 1 above would apply in this case as well.

3. **Scenario 3:**

   A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing risk-based Critical Asset identification methodology and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as risk-based Critical Asset identification methodology. This scenario will be discussed in two sections, the first dealing with the combination of risk-based Critical Asset identification methodologies; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the risk-based Critical Asset identification methodologies: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate risk-based Critical Asset identification methodologies while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate the separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined risk-based Critical Asset identification methodology and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R2 and R3. If additional Critical Assets are identified as a result of the application of the merged risk-based Critical Asset identification methodology, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merge plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated Critical Asset, but no newly designated Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning

Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
R8	24 months	12 months
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[4] Compliance Schedule for Standards CIP-002-2 through CIP-009-2 or CIP-002-3 through CIP-009-3 For Entities Registering in April 2008 and Thereafter					
		Registration + 12 months	Registration + 24 months		
		All Facilities	All Facilities		
CIP-002-2 or CIP-002-3 — Critical Cyber Assets					
All Requirements			Compliant		
Standard CIP-003-2 or CIP-003-3 — Security Management Controls					
All Requirements Except R2			Compliant		
R2		Compliant			
Standard CIP-004-2 or CIP-004-3 — Personnel & Training					
All Requirements			Compliant		
Standard CIP-005-2 or CIP-005-3 — Electronic Security					
All Requirements			Compliant		
Standard CIP-006-2 or CIP-006-3 — Physical Security					
All Requirements			Compliant		
Standard CIP-007-2 or CIP-007-3 — Systems Security Management					
All Requirements			Compliant		
Standard CIP-008-2 or CIP-008-3 — Incident Reporting and Response Planning					
All Requirements			Compliant		
Standard CIP-009-2 or CIP-009-3 — Recovery Plans					
All Requirements			Compliant		

[4] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

~~**Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards**~~

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan ~~identifies~~applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for ~~becoming compliant~~ compliance with the requirements of either Version 2 or Version 3 of the NERC Reliability Standards CIP-003~~-2~~ through CIP-009~~-2~~[1] on Cyber Security for (a) newly Registered Entities and ~~their successor standards, for assets determined to be~~(b) newly identified Critical Cyber Assets ~~once~~by an existing Registered Entity after the Registered Entity's applicable ~~'Compliant'~~*Compliant* milestone date ~~listed in the existing Implementation Plan~~ has already passed.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan ~~specifies only a 'Compliant'~~ defines the *Compliant* milestone~~. The Compliant milestone is expressed~~ date in ~~this Implementation Plan table (Table 2) as the~~ terms of the number of calendar months ~~following the~~after designation of the newly identified ~~asset~~ Cyber Asset as a Critical Cyber Asset, following the ~~requirements of~~ process stated in NERC Standard CIP-002~~-~~. These *Compliant* Milestone dates are included in Table 2 ~~or its successor standard~~of this Implementation Plan.

~~For some~~ The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the risk-based Critical Asset identification methodology. Upon a subsequent annual application of the risk-based Critical Asset identification method in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, and Version 3) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2', or '-3') will be applied to that particular reference.
[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

Table 2 defines the *Compliant* milestone dates for all of the requirements~~, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as '0' herein. For other~~ defined in the NERC Reliability Standards CIP-003 through CIP-009, in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on ~~the Compliant date. These are annotated as *existing*~~its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

~~In all cases where~~A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the *Compliant* milestone ~~for compliance~~date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the *Compliant* milestone date has been reached.

For those NERC Reliability Standard requirements that include a prescribed records retention period (e.g., retention of logs for 90 days), a Responsible Entity is expected to begin collection and retention of the required "data," "documents," "documentation," "logs," and "records" by the *Compliant* milestone date in Table 2.

For retention requirements that are triggered by a specific event (e.g., a reportable incident), collection and retention of the required "data," "documents," "documentation," "logs," and "records" begins with the triggering event. In this instance, the requirement for records collection and retention does not begin until the *Compliant* milestone date in Table 2 is reached and only applies to triggering events occurring after the *Compliant* milestone date.

For those NERC Reliability Standard requirements that do not include a specified ~~(i.e., not annotated as *existing*), the~~ periodicity or records retention requirement, a Responsible Entity is expected to have available all ~~audit~~ records required to demonstrate compliance ~~(i.e., to be~~

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

~~'Auditably Compliant') one year following~~these requirements by the *Compliant* milestone ~~listed~~date in ~~this~~ Table 2.

Implementation Plan~~. Where the milestone assumes prior~~ for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC in April 2008 or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance ~~(i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing~~implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance ~~(i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones~~schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

~~There are no~~Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones ~~specified herein for compliance with NERC Standard CIP-002. All~~defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible ~~Entities are required~~Entity according to ~~be compliant with~~ the process defined in NERC Reliability Standard CIP-002~~ based on the existing Implementation Plan.~~

~~Implementation Schedule~~

~~There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:~~

1. ~~A Cyber Asset becomes the *first identified* Critical Cyber Asset at a responsible Entity~~. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP ~~standards~~-003 through CIP-009, *not due to a planned change~~.~~ in the electric system or*

Cyber Assets by the Responsibility Entity (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP ~~standards~~-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsibility Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

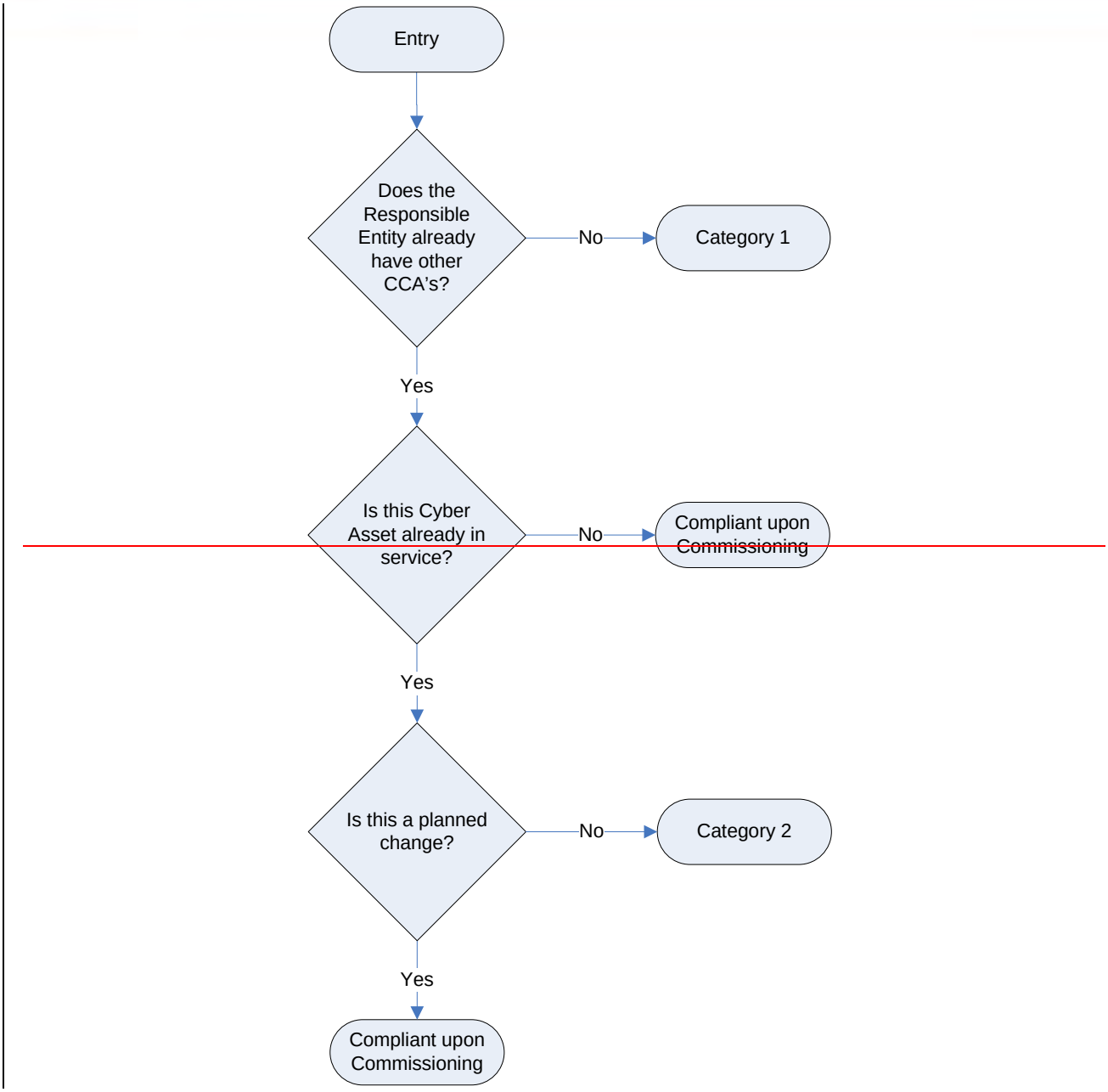
Note that the ~~term~~phrase 'Cyber Asset becomes subject to the ~~CIP standards'~~NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on established criteria or thresholds in the Responsible Entity's existing risk-based Critical Asset identification method (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of that risk-based Critical Asset Identification process is required annually (by CIP-002 R2), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.


Entry
Does the Responsible Entity already have other CCA's?
No
Category 1
Yes
Is this Cyber Asset already in service?
No
Compliant upon Commissioning
Yes
Is this a planned change?
No
Category 2
Yes
Compliant upon Commissioning

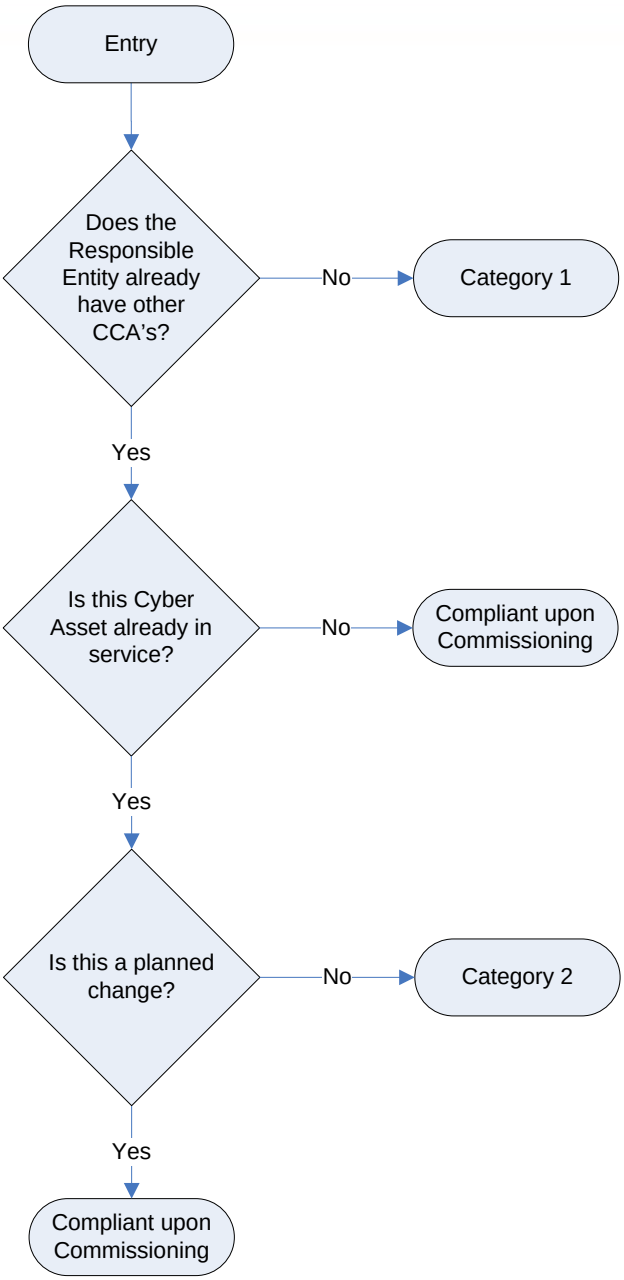


Figure 1: Category Selection Process Flow

~~The individual categories are distinguished as follows:~~

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with ~~-~~Critical Assets, but has now identified one or more Critical Cyber Assets. ~~The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-002-1 through CIP-009-1.)~~ As such, it is presumed that the Responsible Entity ~~has no~~ does not have a previously established ~~cyber security~~CIP compliance implementation program ~~in force. Table 3 also shall apply~~.

~~1.~~The *Compliant* milestones defined for this Category are defined in ~~the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.~~

Table 2 (Milestone Category ~~2~~1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established ~~CIP Compliance~~ NERC Reliability Standards CIP compliance implementation program ~~as required by an existing Implementation Schedule~~in place, and ~~now~~ has ~~added~~ newly identified additional ~~items~~existing Cyber Assets that need to be added to its Critical Cyber Asset list~~. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented~~ and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*~~, not when they are added or modified through construction, upgrade or replacement.~~ as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible

Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

~~In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.~~

~~In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.~~

~~A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.~~

Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established ~~CIP Compliance~~ NERC Reliability Standards CIP compliance implementation program ~~as required by an existing Implementation Schedule~~ and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:
    a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on planning or impact studies) upon its commissioning or activation ~~(e.g., based on planning or impact studies).~~.
    b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset.
    c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset.

d) Planned addition of:
   i. a Critical Cyber Asset, or,
   ii. ~~an other~~another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP ~~Compliance Program as required by an existing Implementation Schedule~~compliance implementation program.

~~This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.~~

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the ~~responsible~~Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

~~Since the assets must be compliant upon commissioning, no milestones are provided herein.~~

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies.

1. **Category 1 Scenario:**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset

   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is the NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology implementation by each predecessor Responsible Entity.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate risk-based Critical Asset identification methodology implementation while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of risk-based Critical Asset identification methodology(ies) as required in CIP-002 R2, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate methodologies, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the risk-based Critical Asset identification methodology as required in CIP-002 R2, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R3. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period),

then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Category 2 Scenario:**

A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology from Scenario 1 above would apply in this case as well.

3. **Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing risk-based Critical Asset identification methodology and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as risk-based Critical Asset identification methodology. This scenario will be discussed in two sections, the first dealing with the combination of risk-based Critical Asset identification methodologies; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the risk-based Critical Asset identification methodologies: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate risk-based Critical Asset identification methodologies while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate the separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity specific circumstances may dictate or allow the two

programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined risk-based Critical Asset identification methodology and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R2 and R3. If additional Critical Assets are identified as a result of the application of the merged risk-based Critical Asset identification methodology, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merge plan' must be made

available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated ~~a~~ Critical Asset, but no newly designated Critical Cyber Assets. This ~~is~~situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with ~~these standards~~the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample ~~situations~~scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No ~~CIP~~ Program (note 1)	Existing ~~CIP~~ Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset ~~–~~ never before in service and not a replacement for an existing Cyber Asset ~~–~~ added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
R8	24 months	12 months
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[4] Compliance Schedule for Standards CIP-002-2 through CIP-009-2 or ~~Their Successor Standards~~CIP-002-3 through CIP-009-3 For Entities Registering in April 2008 and Thereafter					
	~~Upon Registration~~	Registration + 12 months	Registration + 24 months	~~Registration + 36 months~~	
~~Requirement~~		All Facilities	All Facilities	~~All Facilities~~	~~All Facilities~~
CIP-002-2 or CIP-002-3 — Critical Cyber Assets ~~or its Successor Standard~~					
All Requirements		~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-003-2 or CIP-003-3 — Security Management Controls ~~or its Successor Standard~~					
All Requirements Except R2		~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
R2		~~SC~~Compliant	~~C~~	~~AC~~	~~AC~~
Standard CIP-004-2 or CIP-004-3 — Personnel & Training ~~or its Successor Standard~~					
All Requirements		~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-005-2 or CIP-005-3 — Electronic Security ~~or its Successor Standard~~					
All Requirements		~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-006-2 or CIP-006-3 — Physical Security ~~or its Successor Standard~~					
All Requirements		~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-007-2 or CIP-007-3 — Systems Security Management ~~or its Successor Standard~~					
All Requirements		~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-008-2 or CIP-008-3 — Incident Reporting and Response Planning ~~or its Successor Standard~~					
All Requirements		~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-009-2 or CIP-009-3 — Recovery Plans ~~or its Successor Standard~~					

[4] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

All Requirements	~~**BW**~~	~~**SC**~~**Compliant**	~~**C**~~	~~**AC**~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for Project 2009-21: Cyber Security Ninety-day Response

Please **DO NOT** use this form. Please use the electronic comment form located at the link below to submit comments on the proposed revisions of CIP-002-2 through CIP-009-2, the Implementation Plan for Version 3 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, developed by the standard drafting team as part of Project 2009-21 Cyber Security Ninety-day Response. Comments must be submitted by **November 12, 2009**. If you have questions please contact Joe Bucciero at joe.bucciero@gmail.com or by telephone at (267) 981-5445.

http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

Background Information

On May 22, 2009, NERC in its capacity as the Electric Reliability Organization (ERO) filed eight revised CIP Reliability Standards, the Implementation Plan for Version 2 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for approval with the Federal Energy Regulatory Commission (FERC or the Commission), to protect the Bulk-Power System from malicious or unintentional cyber events. The revised CIP Reliability Standards require Bulk-Power System users, owners, and operators to establish a risk-based assessment methodology to identify critical assets and the associated critical cyber assets essential to the critical assets' operation. Once the critical cyber assets are identified, the CIP Reliability Standards require, among other things, that the Responsible Entities establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. The eight CIP Reliability Standards are as follows:

> CIP-002-2 – Cyber Security – Critical Cyber Asset Identification: Requires a Responsible Entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.
>
> CIP-003-2 – Cyber Security – Security Management Controls: Requires a Responsible Entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1.
>
> CIP-004-2 – Cyber Security – Personnel and Training: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.
>
> CIP-005-2 – Cyber Security – Electronic Security Perimeter(s): Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002-1.
>
> CIP-006-2 – Cyber Security – Physical Security: Requires a Responsible Entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

CIP-007-2 – Cyber Security – Systems Security Management: Requires a Responsible Entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

CIP-008-2 – Cyber Security – Incident Reporting and Response Planning: Requires a Responsible Entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

CIP-009-2 – Cyber Security – Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

On September 30, 2009 the Commission approved Version 2 of the CIP Reliability Standards with an effective date of April 1, 2010. In its September 30, 2009 order (Order RD09-7), the Commission directed NERC to make additional changes to two of the standards (CIP-006-2 and CIP-008-2) and the associated implementation plan. The order directed NERC to file the modified standards and Implementation Plan within 90 days and, among other things, required the following modifications:

- A modification to Reliability Standard CIP-006-2 – Cyber Security — Physical Security to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit.
- A modification to Reliability Standard CIP-008-2 – Cyber Security — Incident Reporting and Response Planning, Requirement R1.6 to remove the last sentence of CIP-008-2 Requirement R1.6.
- A revised Version 2 Implementation Plan addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to the September 30 Order.

Although the Commission directed changes to only two of the eight (CIP-002-2 thru CIP-009-2) reliability standards, conforming changes are proposed for the remaining six CIP Reliability Standards (CIP-002-2 through CIP-005-2, CIP-007-2, and CIP-009-2) to correct the cross references within the set of standards. If left untouched, the Purpose statements and many requirements within the set of standards would be incorrect as they all reference CIP-002-2 through CIP-009-2.

The Implementation Plan is presented in two documents. One document addresses the Implementation Plan related to the specific version (Version 3) of the CIP Reliability Standards. The second document is meant to be a stand-alone, free-standing Implementation Plan that survives the versioning of the CIP Reliability Standards and addresses the implementation of Newly Identified Critical Cyber Assets and Newly Registered Entities that may occur over the life of these standards. Although the Commission directed that the Implementation Plan documents be combined to avoid confusion, the Standard Drafting Team believes that each document has its specific purpose, and instead, chose to clarify the content of each document to remove the confusion identified by the Commission in Attachment, "Compliance Issues on Implementation Plan", to Order RD09-7.

Since NERC is required to respond to the Commission's directive within 90 days, the Standard Authorization Request (SAR) and the proposed modifications to the standards and implementation plan are being posted simultaneously to expedite the process.

(Note: In its May 22, 2009 filing of the version 2 CIP standards, NERC inadvertently left off the approved interpretation of CIP-006-1a. The interpretation for CIP-006-1a is added back in for this set of proposed changes to create CIP-006-3a.)

Questions

Your responses to the following questions will assist the SDT for Project 2009-21 Cyber Security Ninety-day Response in finalizing the work for CIP-002-3 through CIP-009-3 relative to the proposed modifications summarized above. For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

1. In its order approving CIP-002-2 through CIP-009-2, the Commission directed NERC to make changes to CIP-006-2 and CIP-008-2 as well as the implementation plan for newly identified critical cyber assets and file those changes within 90 days of the order. Do you agree that the SAR accurately addresses the scope of these directives? If not, please identify what you feel is missing in the SAR.

   ☐ Yes

   ☐ No

   Comments:

2. Do you agree that the proposed modifications to CIP-006-2, CIP-008-2, and the implementation plans meet the intent of the Commission's directives? If not, please identify what changes you feel are needed to meet the intent of these directives.

☐ Yes

☐ No

Comments:

3. Do you have any additional comments associated with the proposed SAR for Project 2009-21: Cyber Security Ninety-day Response? If yes, please explain.

☐ Yes

☐ No

Comments:

4. Do you have any additional comments associated with the proposed CIP-006-2, CIP-008-2, and the implementation plans? If yes, please explain.

☐ Yes

☐ No

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Comment Period Open
October 13–November 12, 2009

Now available at: http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

Project 2009-21: Cyber Security Ninety-day Response

The drafting team for this project is seeking comments on the following documents **until 8 p.m. EST on November 12, 2009**:

- Standards Authorization Request (SAR) for Project 2009-21 Cyber Security Ninety-day Response
- Proposed Critical Infrastructure Protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3 (version 3 CIP standards), including associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs)
- Implementation Plan for the Version 3 CIP standards
- Revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Instructions

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at Lauren.Koller@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page: http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

Next Steps

The drafting team will draft and post responses to comments received during this period. Then, as directed by the NERC Standards Committee during its October 7-8, 2009 meeting, the standards and implementation plans will be posted for ballot (with no pre-ballot review period) so that NERC can comply with the Federal Energy Regulatory Commission (FERC) directive issued in its September 30, 2009 order to develop and file modifications to the CIP Reliability Standards within 90 days of the date of the order.

Project Background

The purpose of this project is to modify certain CIP Reliability Standards in response to the directives issued in the FERC September 30, 2009 *Order Approving Revised Reliability Standards For Critical Infrastructure Protection And Requesting Compliance Filing*: http://www.nerc.com/files/OrderApproving_V2_CIP-002_CIP-009-09302009.pdf

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator

Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

Standards Development Process

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

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Individual or group. (29 Responses)
Name (18 Responses)
Organization (18 Responses)
Group Name (11 Responses)
Lead Contact (11 Responses)
Question 1 (28 Responses)
Question 1 Comments (29 Responses)
Question 2 (28 Responses)
Question 2 Comments (29 Responses)
Question 3 (29 Responses)
Question 3 Comments (29 Responses)
Question 4 (29 Responses)
Question 4 Comments (29 Responses)

Individual
Jim Lauth
Silicon Valley Power
Yes
Yes
No
Yes
Violastion Severity Levels in some cases do not provide for either Moderate or Low levels in all cases
Individual
Jeremy Bergstrom
Navasota Odessa Energy Partners, LP
Yes
Yes
No
No
Group
Exelon
Laurie Urbancik
Yes
No
We do not agree with the CIP-006-3 R1.6 change where you have included the requirement for the visitor log to contain "...the identity of personnel with authorized, unescorted physical access performing the escort." This would be an excessive administrative burden that goes beyond what FERC ordered in paragraph 30 which simply stated "...the commission directs the ERO to develop a modification to Reliability Standard CIP-006-2, through the NERC Reliability Standards development process, to add a requirement on visitor control programs, including the use of

visitor logs to document entry and exit, within 90 days of the date of this order". Your additional requirement can be interpreted to mean any hand off of escort responsibilities would also need to be documented which would be an excessive administrative burden that would provide no additional assurances or security. An acceptable alternative would be for the visitor log to include a reference to the site contact and reason for the visit. These are things known at the time of visitor sign in which would not require additional updates through out the time the visitor remains within the secure area.
No
No
1) For the “Implementation Plan for …Newly Registered Entities”, we suggest the that the last two sentences in the second paragraph under the Category 1 Scenario beginning with following language should be deleted: “it would be preferred that a single program be the result of this analysis, however”. 2) For the “Implementation Plan for …Newly Registered Entities”, we suggest that the last two sentences of the Scenario 3, (a) paragraph be deleted: “It would be preferred that a single program be the result of this analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.”
Individual
Kasia Mihalchuk
Manitoba Hydro
Yes
No
The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was modified beyond the Commision's directives in RD09-7-000. See response to Question 4.
No
Yes
The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was significantly changed after approval by industry and the NERC BOT. The changes, pertaining to periodic requirements, were not directed by FERC in Order 706 or Order RD09-7-000, or through industry comments. The changes require that for a number of requirements, which were not specified by NERC, with “… a prescribed periodicity… the first occurrence of the recurring requirement must be completed by the Compliant milestone date…”, which could advance the need to meet the requirements up to a year. This is not the general understanding of the industry, and was not the guidance provided in the NERC (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1. From the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 document provided with the Version 1 standards, “Compliant means that the entity meets the full intent of the requirements, and is beginning to maintain required “data”, “documents”, “logs”, and “records”. Auditably Compliant means that the entity meets the full intent of the requirements and can demonstrate compliance to an auditor, including 12-calendar-months of auditable “data”, “documents”, “logs”, and “records”.” Meeting the intent of the requirements means that the processes, procedures and infrastructure are in place to begin collecting data during the Auditably Compliant period. A quarterly review should not need to be conducted before the Compliant date; it is completed, at latest, at the end of the first quarter of the compliance period. The direction provided in the new Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is unclear and inconsistent, as some unspecified requirements with a prescribed periodicity must have their first periodic occurrence completed by the compliance date, while other unspecified periodic requirements can begin collection of their respective data by the compliance date. It is too late to introduce new compliance direction for standards whose initial compliance dates will have passed by the time the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is approved. We recommend the removal of the paragraph on Page 2 which begins “A number of the NERC Reliability Standard requirements include a prescribed periodicity …”. With the removal of that paragraph, the following paragraphs in that section are unnecessary and should also be removed.
Individual
Michael Puscas
The United Illuminating Company
Yes
Yes

No
No
Individual
James Starling
South Carolina Electric and Gas
Yes
Yes
Order No. 706-B Nuclear Implementation schedule should be added to the implementation table for the proposed modifications to CIP-006-2, CIP-008-2 in order to avoid any confusion between the two schedules.
No
No
Individual
Steve Newman
MidAmerican Energy Company
Yes
Yes
No
Yes
Implementation plan for Newly Identified Critical Cyber Assets: MidAmerican appreciates the specificity in the implementation plan for newly identified Critical Cyber Assets, identified under table 2. Four paragraphs (periodicity or recurrence of the requirement activity, prescribed record retention periods, specific event triggered requirements and records to demonstrate compliance when there is no specified periodicity) provide clarification. Newly Registered Entity Scenarios, Scenario 3a: When combining separate risk-based methodologies, a methodology that provides the most robust level of protection against a cyber attack should be selected. The resulting methodology should be applied to the combined system with no requirement that the resultant list contain all of the critical assets previously identified by the two separate methodologies.
Group
PacifiCorp
Sandra Shaffer
Yes
Yes
Yes
Comments: PacifiCorp generally supports the Request for Rehearing or Clarification submitted by the Edison Electric Institute (EEI) submitted in FERC Docket No. RD09-7 on October 30, 2009. Specifically, PacifiCorp agrees with EEI that the ninety-day deadline imposed by FERC's September 30, 2009 to modify the CIP Reliability Standards is unreasonably short. In addition, PacifiCorp is concerned that this type of unreasonable deadline threatens to undermine NERC's standards development process. Currently, the NERC standards development process is the only opportunity for industry stakeholders to participate in the development of reliability standards that will have significant operational and business impacts. Unreasonable deadlines set by FERC and the corresponding "expedited" standards development process threatens to undermine the robustness of the current process. While PacifiCorp does not have substantive issues with the current proposed changes, it is concerned regarding the procedure being used here to adopt these changes.
Yes
Regarding the implementation plan treatment of merging Responsibilities Entities: when combining separate risk-based methodologies, PacifiCorp believes that each separate methodology should be applied to the combined system and the methodology that provides the most robust level of protection against a cyber attack based on the critical assets identified

should be selected. The selected methodology should be applied to the combined system with no requirement that the resultant list contain all of the critical assets previously identified by the two separate methodologies.
Group
Northeast Power Coordinating Council
Guy Zito
Yes
No
CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – "Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor." CIP-006 R1.6.2 should be modified to "Requirement for continuous escorted access of visitors within the Physical Security Perimeter." The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For additional information see the response to question 4.
Yes
Development of this SAR should follow the approved SAR process.
Yes
In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph: "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached." should be deleted for the following reasons: • It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. "at least annually"), an entity understands that the Responsible Entity is compliant with the requirement if it can demonstrably produce completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example), and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually. CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan. CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at the Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. • It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order." This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Individual
Marty Berland
Progress Energy

No
Yes
Progress Energy intends to vote Negative in the upcoming ballot primarily because it disagrees with the proposed language in CIP-006-3a, R1.6.1. Specifically, Progress does not agree with the requirement to document the visitor's time and date of exit from Physical Security Perimeters. Progress is aware of the FERC order issued September 30, 2009 which requires logging of entry and exit dates and times for escorted visitors. Nevertheless, as a practical matter, for facilities with multiple PSPs such as large power plants, it is not feasible to maintain visitor logs for egress when frequent daily or hourly entries to/exits from such PSPs occur, such as during an outage. More importantly, Progress believes that the value of an authorized escort is to maintain continuous surveillance, accountability, and control over the visitor whenever the visitor is within the PSP. Requiring the logging of egress dates and times for escorted visitors does not provide any additional CIP benefit because it does not improve the security of the PSP in real time. It would, however, greatly increase cost, reduce productivity, and create opportunity for inadvertent violation of the NERC requirement. FERC did not order that personnel with unescorted access also be required to log egress times and dates, presumably because there is no benefit to doing so. Likewise, if the escort is properly performing his/her function, there would be no reason to log egress times and dates for those being escorted.
Individual
Randy Schimka
San Diego Gas and Electric Co
Yes
While the SAR does accurately address the scope of the FERC directives, we would suggest that the SAR's name be changed to something more descriptive than "Cyber Security Ninety-Day Response" to make it easier to locate and understand in the future. Perhaps a SAR title like "NERC response to FERC Cyber Security V2 Std Approval" would help to make the contents clearer when searching or browsing in the future.
No
CIP-008-2: We are in agreement with the proposed modifications to CIP-008-2. CIP-006-2: In the modifications made to CIP-006-2, we have an issue with the language requiring the documentation of "entry to and exit from Physical Security Perimeters." Many badging systems document personnel ingress to PSP areas, but not egress and some entities may utilize their badging system to track visitors (visitors swipe for record keeping purposes but their badge cannot open any access points). A recent interpretation of CIP-006 also confirmed that only ingress monitoring is required, and that is the functionality delivered by many badge access systems. After their visit is completed, a visitor typically signs out at the central Security Station and surrender their visitor badge at that time. In order to make the R1.6 language more easily understood, our first preference would be to remove the "and exit from" language. If that cannot be done, then our second preference would be to change the language in R1.6.1 to "date of entry to and last exit of the day from Physical Security Perimeters". Manually logging all visitor ingress and egress from CCA areas could be potentially very time-consuming without providing additional reliability to the Bulk Electric System. Implementation Plans: In the Implementation plan language, we were looking for particular guidance showing how an asset would be treated if acquired from a third party. In particular, there could be a scenario where the current owner does not list any critical assets or critical cyber assets. Once the acquisition takes place, what accommodations should be made in the implementation plan if the new owner feels that there are critical assets or critical cyber assets associated with the asset? It could theoretically take a considerable amount of time to start a proper Cyber Security program for the acquired plant from scratch. A 12 month implementation plan schedule may not be practical given the complexity of assessing the acquired plant and making the necessary cyber security modifications and additions for Compliance. We'd like to suggest that a 24 month implementation plan schedule would be more appropriate in cases like this.
No
No
Group
Dominion Virginia Power
Ruth Blevins
Yes
Yes

No
Yes
The proposed requirement CIP-006-3a R1.6.1 is redundant to and/or conflicts with requirement R6. A suggested modification: R1.6 Each PSP shall be governed by a visitor control program which, at a minimum, provides the following requirements: R1.6.1 Continuous escorting of any personnel without authorized unescorted access to the PSP R1.6.2 Meets the logging requirements found in CIP-006-3a R6. If the above change is not considered, please amend CIP-006-3a R6 to indicate that it only applies to non-visitors.
Individual
James H. Sorrels, Jr.
American Electric Power
Yes
Yes
No
No
Individual
Patrick Brown
PJM Interconnection
Yes
Yes
No
Yes
Comments: PJM would like to request clarification on the meaning of "identity" in CIP 006-3, Requirement R1.6.1; "Visitor logs to document visitor's identity, time and date of..." It is not clear, if the logs should only contain the visitor's name or it should require some form of verification of his/her identity, such as, a government (federal or local) issue photo ID. PJM is in agreement with a "Medium" VRF for standard number "CIP-006-3a", Requirement number "R1.6.1", if the clarification of "identity" represents the verification of the individuals identity; however, if the clarification of "identity" means, that the log should only contain "name only", PJM suggest the VRF of "Low".
Group
BGE CIP Core Team
Ed Carmen
Yes
Yes
No
Yes
1. Clarification is needed on how to apply a visitor control program for PSPs that have been established at a cabinet level (e.g., CCAs, or equipment treated as a CCA per CIP requirements, are housed within a secured cabinet that is located within a data center, and they are the only CCAs within the data center. Access to the cabinet that houses the CCAs is controlled, and therefore the cabinet serves as the PSP for these cyber assets)? 2. What is the implementation plan for the CIP Version 3 Reliability Standards?
Individual
Adam Menendez
Portland General Electric Company
No
No

No
Yes
The Draft Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities contains the following statement: "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." PGE strongly disagrees with this approach. PGE believes that this language directly contradicts the plain language understanding of an “annual” requirement, and this is made clear by reference to the Standards currently under consideration. Looking at Standard CIP-003-3 R4 (Information Protection), for example, a Responsible Entity “shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.” It is clear, then, that a Registered Entity must have in place an Information Protection Program on or before the “Compliant” milestone date. However, R4.3 of this Standard provides that 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.” (Emphasis added.) This R4.3 clearly contemplates an “assessment” of the information protection program that takes place after the initial implementation of that program and recurs “annually” thereafter. Applying the interpretation of “annual” set forth in the Draft Implementation Plan to this Standard, an entity would have to “implement and document” a program, and also “assess adherence” to that same program by the “Compliant” milestone date. Determining adherence to a new program requires that the program be in place and exercised for a period of time, otherwise you do not have enough relevant data to “assess adherence”. Similarly, in Standard CIP-007-3 R8 (Cyber Vulnerability Assessment), a Responsible Entity “shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually.” Looking at the sub requirements within this R8, it is clear that this “annual” review requirement is triggered after the “Compliant” milestone date. Requirement 8.2, for example, requires the entity to “verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled.” This requirement pertaining to ports and services is set forth separately in R2 of the same Standard. As such, the plain language interpretation of this Standard is that an entity must establish compliance with the stand-alone R2 requirement pertaining to ports and services on or before the “Compliant” milestone date, and then perform a Cyber Vulnerability Assessment annually thereafter to test ongoing compliance. If the Cyber Vulnerability Assessment (R8) must be performed for the first time on or before the “Compliant” milestone date, then it is duplicative of other requirements within the Standard. It is clear, then, that a requirement to perform an action on an annual basis gives the entity a year from the time that the requirement reaches the Compliant milestone date for the first instance of performing that action. The Standard Drafting Team's approach would require a utility to comply with the requirement before the Compliant milestone date, rendering the Compliant milestone date meaningless. An entity has not failed to meet the requirement until it fails to complete the requirement activity on an annual basis. By definition this cannot take place until two conditions have been met: (1) the requirement has been mandatory on the entity (i.e., at the Compliant stage); and (2) the entity has failed to perform the requirement activity at least as often as once a year. The entity's failure to perform the activity prior to expiration of the “annual” period following the Compliant milestone cannot constitute noncompliance because the activity can still be taking place on an annual basis. Construing all requirements with a prescribed periodicity to require the first performance of the requirement activity prior to the Compliant milestone can undermine the intent of the standard, which is for the registered entity to perform the activity in keeping with their typical annual performance cycles. For example, a requirement that reaches the "Compliant" milestone on January 1 can include an annual performance activity that the entity typically does as part of an outage drill which is done every September. The entity should not be forced to alter their typical annual schedule in order to meet the requirement before it has reached the "Compliant" stage. This approach is not supported by past standard development activity or by FERC Order and represents a fundamental shift in NERC's approach to such requirements with prescribed periodicities. Given that many such requirements are currently or will soon be at the Compliant milestone date, such a shift in approach would require adequate notice to the affected entities.
Individual
Martin Bauer
US Bureau of Reclamation
Yes
We applaud the SDT in following the standards development process by submitting an implementaton plan that addresses the Commissions order. This is consistent with the Commissions requirement that "We direct NERC to submit, within 90 days of the date of

issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order" it is also consistent with the process for submitting revision (Reference 16 USC Sec. 824o (d) (5) The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.)
Yes
No
No
Individual
Terrence Walsh
Consolidated Edison Company of New York INC.
Yes
No
CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – "Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor." We suggest: "R1.6.1. Visitor logs (manual or automated) to identify visitors, the purpose of the visit, the date and time of entry and exit from the Physical Security Perimeters, and to identify personnel with authorized, unescorted physical access performing the escort." CIP-006 R1.6.2 should be modified to "R1.6.2. Requirement for continuous escorted access of visitors within the Physical Security Perimeter." The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For more information see the answer to question 4.
Yes
Development of this SAR should follow the approved SAR process
Yes
In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached." Should be deleted for the following reasons: • It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. "at least annually"), an entity understand that the Responsible Entity is compliant with the requirement if it can produce demonstration of completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example) and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually. CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan. CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at Compliant date, and should only be required to produce records and

logs of the first periodic requirement after the Compliant date. • It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order." This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Group
FirstEnergy
Sam Ciccone
Yes
We commend NERC for their expedient response to FERC's directives.
Yes
Yes
We understand that NERC is merely responding to directives with a specific completion time frame of 90-days. And we believe that NERC has done this job well. Unfortunately, due to the short 90-day time frame, NERC and its stakeholders did not have much time to challenge FERC's directives. We offer the following as strictly comments on the directive to modify CIP-008: CIP-008 – Req. R1.6 – FERC feels that the statement "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test" should be removed and NERC has proposed to remove it per the directive by FERC. It is interesting to note that in Order 706 par. 687, FERC stated "the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise." Yet, in the recent Order, per par. 38, FERC has directed NERC to remove this statement and stated in their determination "we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement". It appears that FERC may have inadvertently sent unclear and inconsistent messages when it said "the ERO should clarify" in Order 706, and then asked NERC to remove the statement in the recent Order because it is merely a "clarification of the requirement". It is not clear how removing this statement makes R1.6 a better requirement since, as FERC says, "...it is similar to an interpretation or clarification of a requirement." In addition, the phrase, "A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise..." is also a clarifying statement and the FERC raised no concern over its inclusion in this standard requirement. The direction to remove clarifying statements seems to go against the goal of writing clear and concise reliability standards.
Yes
CIP-007 – Per NERC Project 2009-16, the stakeholders and NERC's Board recently approved an interpretation of Req. R2 to clarify that the meaning of ports in this requirement is referring to "logical" ports. NERC may want to consider adding this interpretation to CIP-007 Version 3 so that it gets incorporated into the standard expediently rather than wait until a later time. Waiting until a later time will require both another revision to the standard and an extra filing by NERC to add the interpretation.
Individual
Edward Bedder
Orange and Rockland Utilities Inc
Yes
No
CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor. We suggest: R1.6.1. Visitor logs (manual or automated) to identify visitors, the purpose of the visit, the date and time of entry and exit from the Physical Security Perimeters, and to identify personnel with authorized, unescorted physical access performing the escort. CIP-006 R1.6.2 should be modified to R1.6.2. Requirement for continuous escorted access of visitors within the Physical Security Perimeter. The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably

Compliant milestone. These words are not in any FERC Order or Directive. For more information see the answer to question 4.
Yes
Yes
In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph states: A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required “data,” “documents,” “documentation,” “logs,” and “records” to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached. This statement should be deleted for the following reasons: • It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. “at least annually”), an entity understand that the Responsible Entity is compliant with the requirement if it can produce demonstration of completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example) and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually. CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan. CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. • It is outside of the scope of the SAR. In its Order, the FERC’s directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: “We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order.” This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Group
Transmission Owner
Silvia Parada-Mitchell
No
Generally we agree with the proposed changes. However, one area of concern is CIP-006-2. We feel that it should not be a requirement for persons with unescorted physical access to have to swipe out when leaving the PSP. Swiping in should be sufficient.
No
In reading the second sentence of the New Asset Implementation Plan redline which starts, "In those instances…" it seems that this is stating that an entity must demonstrate compliance prior to the actual Compliant date set forth in the current implementation plan. The implementation plan right now states that the period of time between the Compliant date and Auditably Compliant date is when you must start keeping records, logs, documents, etc. If the current proposal goes through, the entity would need to conduct its first vulnerability assessment sometime prior to the Compliant date. This is a huge shift and shortens the implementation window up to a year. Hence, we feel this change should not be approved.
Yes
Although the SAR proposes many changes, these changes lead to ambiguity and this ambiguity lends more latitude to the regions.
Yes
Regarding CIP-006-3a, R1.6.1 specifically, we do not agree with the requirement to document the visitor’s time and date of exit from Physical Security Perimeters. Facilities with multiple PSPs

such as large power plants, it is not feasible to maintain visitor logs for egress when frequent daily or hourly entries to/exits from such PSPs occur, such as during an outage. We believe the value of an authorized escort is to maintain continuous surveillance, accountability, and control over the visitor whenever the visitor is within the PSP. Requiring the logging of egress dates and times for escorted visitors does not provide any additional CIP benefit because it does not improve the security of the PSP in real time. It would, however, greatly increase cost, reduce productivity, and create opportunity for inadvertent violation of the NERC requirement.
Group
E.ON U.S. LLC
Brent Ingebrigtson
Yes
No
In paragraph 29 of the Order, the Commission approves version 2 of the standard on the basis that continuous is analogous to supervised. Furthermore, the Commission states as its goal that Responsible Entities implement visitor control programs and be able to reasonably demonstrate that they maintain such programs. The order reiterates that the Version 2 standards achieve this goal. The proposed changes to CIP-006-2 do not meet the Commission's goal because of prescriptive measures that do not allow for reasonable demonstration
No
Yes
Modify requirement R1.6.1 to read as follows: R1.6.1 Visitor logs. Utilizing less prescriptive language in this requirement will provide Responsible Entities with the flexibility to reasonably apply the standard to each of the various circumstances that exist in the industry. For example, providing continuous escorts for parties that don't have unrestricted access to the critical cyber equipment or facilities requires additional staffing. Due to, for example, the number of potential contractors that may be "on-site" at any given time, numerous escorts may be required. The use of a "monitor" would not be sufficient because the escort must have enough knowledge to determine if a cyber incident is occurring. E.ON U.S. favors a process whereby contractors procure critical access certification from NERC or the RRO.
Group
NextEra Energy Resources
Benjamin Church
No
Generally we agree with the proposed changes. However, one area of concern is CIP-006-2. We feel that it should not be a requirement for persons with unescorted physical access to have to swipe out when leaving the PSP. Swiping in should be sufficient.
No
In reading the second sentence of the New Asset Implementation Plan redline which starts, "In those instances…" it seems that this is stating that an entity must demonstrate compliance prior to the actual Compliant date set forth in the current implementation plan. The implementation plan right now states that the period of time between the Compliant date and Auditably Compliant date is when you must start keeping records, logs, documents, etc. If the current proposal goes through, the entity would need to conduct its first vulnerability assessment sometime prior to the Compliant date. This is a huge shift and shortens the implementation window up to a year. Hence, we feel this change should not be approved.
Yes
Although the SAR proposes many changes, these changes lead to ambiguity and this ambiguity lends more latitude to the regions.
Yes
Regarding CIP-006-3a, R1.6.1 specifically, we do not agree with the requirement to document the visitor's time and date of exit from Physical Security Perimeters. Facilities with multiple PSPs such as large power plants, it is not feasible to maintain visitor logs for egress when frequent daily or hourly entries to/exits from such PSPs occur, such as during an outage. We believe the value of an authorized escort is to maintain continuous surveillance, accountability, and control over the visitor whenever the visitor is within the PSP. Requiring the logging of egress dates and times for escorted visitors does not provide any additional CIP benefit because it does not improve the security of the PSP in real time. It would, however, greatly increase cost, reduce productivity, and create opportunity for inadvertent violation of the NERC requirement.
Individual
Greg Rowland
Duke Energy

Yes
Yes
No
Yes
We support the MISO Standards Collaborators' comments, and have the following additional comments: 1. NERC: V3 Implementation Plan: The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard. Can the industry have some kind of an estimate as to when that will be? 2. Implementation Plan for Newly Identified Critical Assets. Comment/question to NERC. Utilities really want to do the right thing. It is quite possible that new Critical Assets may be identified late in 2009. CIP version 1 has no implementation plan for such new identified Critical Assets, and NERC acknowledges this “compliance gap”. An implementation plan to address this gap is being proposed here. This same implementation plan was proposed in v2. A compliance gap exists for newly identified CA until this proposed effective date. This implementation plan for newly identified Critical assets is desperately needed by the utility. The implementation plan was poorly written when submitted by NERC to FERC and was, therefore, not included in the FERC approved Version 2 materials. This is no fault of the utilities. What is the proposed effective date of the Implementation Plan for Newly Identified Critical Assets? If a utility has newly identified Critical Assets between the compliance date for CIP version 1 and the effective date of the Implementation Plan for Newly Identified Assets, what schedule should they follow for the implementation of CIP? It is not reasonable to expect that newly identified Critical Assets are immediately “auditably compliant” under CIP version 1. What remedy is available to the utilities short of non-compliance related to newly identified Critical Assets prior to the effective date of this Implementation Plan? 3. Version 1 Implementation Plan Retirement: “The Version 1 Implementation Plan will be retired once all Entities in Tables 1, 2, and 3 of that plan have achieved their Compliant state.” The wording in the NERC material states that Version 1 Implementation Plan will not be retired until the Entities achieve compliant state. Is this true? Shouldn’t the posting read “Version 1 Implementation Plan will be retired once the target dates explained in the Phased In Plan expire”? 4. Dropping “Auditably Compliant”. The term “auditably compliant” has been dropped from this future version of the implementation plan. We do not object, but we have a clarifying question: Auditably compliant referred to the need to have 12 months of data. At what point is the utility expected to have 12 months of data accumulated for review during an audit? Is it at the compliant stage or 12 months subsequent to compliant stage?
Individual
Roger Champagne
Hydro-Québec TransÉnergie (HQT)
Yes
No
CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission’s Determination – “Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor.” CIP-006 R1.6.2 should be modified to “Requirement for continuous escorted access of visitors within the Physical Security Perimeter.” The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says “In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2.” We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For additional information see the response to question 4.
Yes
Development of this SAR should follow the approved SAR process.
Yes
In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph: “A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required “data,” “documents,” “documentation,” “logs,” and “records” to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached.” should be deleted for the following reasons: • It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. “at least annually”), an entity

understands that the Responsible Entity is compliant with the requirement if it can demonstrably produce completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example), and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually. CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan. CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at the Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. • It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order." This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.

Individual

Dan Rochester

Independent Electricity System Operator

Yes

No

CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – "Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor." CIP-006 R1.6.2 should be modified to "Requirement for continuous escorted access of visitors within the Physical Security Perimeter." The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For additional information see the response to question 4.

Yes

Development of this SAR should follow the approved SAR process.

Yes

In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph: "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached." should be deleted for the following reasons: • It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. "at least annually"), an entity understands that the Responsible Entity is compliant with the requirement if it can demonstrably produce completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example), and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually. CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan. CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that

require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at the Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. • It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order." This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.

Individual

Jason Shaver

American Transmission Company

Yes

ATC agrees that the SAR reflects the Commission's directive but we do not agree with all of the proposed changes. (Please see our specific comments in the other questions.)

Yes

ATC does not agree with the deletion of the following sentence from CIP-008-2 R1.6 "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test". Although, ATC believes that FERC is correct in its assessment that the sentence could be inferred by Requirement 1 and Requirement 1.6, it does not harm the requirement in any way by remaining part of the standard and should not be deleted. The Commission goes as far as to say that the sentence is similar to an interpretation, so, if that is the case, we don't see any harm in keeping it as part of the standard. Lastly, ATC is concerned that we could be back to this same spot if an entity requests a formal definition of this requirement. From the SDT perspective, what issues are being addressed by removing this sentence? Does the SDT believe that the deletion of this specific sentence will not require the removal of equipment in order to be in compliance with the standard? ATC believes that the sentence does provide additional clarity of the requirements and does not harm reliability and, therefore, should not be removed from the standard. As the Commission clearly points out, this sentence does provide an interpretation or clarification of the standard which the Commission did not disagree. If the SDT does remove this sentence, then we request the SDT to identify any concerns or issues with the interpretation or clarification. (Deleted Sentence) Specifically, would the SDT give an alternate interpretation of this requirement?

No

Yes

Implementation Plan Comments: Item 1: What does the word "compliant" mean when used in the phrase "when Registered Entities has been required to be compliant with NERC Reliability Standard CIP-002"? Does the team mean the "compliant" phase identified in the Original CIP Implementation plan? or, Does the team mean when an entity had to be either "substantially compliant" or "auditable compliant"? The Version 1 Implementation plan identifies three compliant phases. Substantially Compliant Compliant Auditable Compliant Item 2: Question about the last paragraph on page 3: ("For example, if a particular transmission substation has been designated…") This example is structured around the premise that an entity has identified a Critical Asset but has not identified any associated Critical Cyber Asset and seems to point to scenario 3. Is this an example for scenario 3? If so, the SDT should insert an affirmative sentence linking it to scenario 3. Item 3: Question about paragraph 2 on page 4: ("If, however, a particular transmission substation with Cyber Assets does not …") What scenario (1, 2 or 3) is this paragraph attempting to address? It seems that it may be attempting to provide an example of scenario 2 and, if so, we would suggest that the SDT provide a specific sentence linking it to a specific scenario. Item 4: Comment on Figure 1: (Category Selection Process Flow) ATC is concerned that the flow chart is assigning a new requirement for CIP-002-2 requirement 1. Based on the proposed flow chart, it seems that an entity has to determine prior to commissioning, any planned changes that would place a facility on an entity's Critical Asset list. We believe that the flow chart should be modified to state that a planned change to a known Critical Asset has to be Compliant upon commissioning and that a planned change which causes

an existing facility to be placed on the Critical Asset list be allowed to follow Category 2. This additional clarity would address our concern of pre-determination of a Critical Asset for all planned changes. Would an entity be non-compliant if following a completion of planned change the entity subsequently determines that the facility is a Critical Asset? We are asking this question because the flow chart seems to be indicating that entities have to determine Critical Asset prior to commissioning, and if they determined later that a facility is a Critical Asset that entity could be found non-compliant. ATC suggest the following changes: Clarify that for existing Critical Assets any changes to its associated Critical Cyber Assets shall be compliant upon commissioning. Any newly identified Critical Assets will have to follow Category 2 for its associated Critical Cyber Assets. We believe that this change would accurately align with the existing CIP standards. Comments on the Category X (1, 2 and 3) Scenarios: (Page 6 and 7) The SDT has identified three Scenarios a) Category 1 Scenario, b) Category 2 Scenario, and c) Compliant upon Commissioning. Are these scenarios meant to be examples or does the SDT intend on these being specific scenarios meant to define Figure 1? Item 5: Second paragraph page 10: ("Registered Entities are encouraged when combining separate risk-based…") ATC believes that the proposed Implementation plan needs to contain a qualifying statement that the annual application of an entities risk-based assessment methodology allows for the addition or removal of Critical Assets. Standard CIP-002 allows an entity to update its list based on the application of the risk-based assessment methodology and does not require a demonstration of "extraordinary circumstances" for removing a previously identified Critical Asset from its list. We believe that this statement is inserting additional compliance obligations that are not contained within the standard. Suggested Modification: Delete the first sentence. If the SDT does not agree with our suggestion, they need to indicate the language contained within CIP-002 which supports the inclusion of phrase "demonstrate extraordinary circumstances" within the standard. Item 6: Table 1: ATC does not believe that enough clarity exists between the phrase Existing Asset and Planned modification. Is a company non-compliance with CIP-002 if a planned modification becomes a Critical Asset following commissioning? (Example: An upgrade is made to an existing asset and it was not identified previously as a Critical Asset. Following commissioning: During the annual application of an entity's risk-based assessment methodology the new asset is identified as a Critical Asset. Does category 2 apply?) Item 7: Table 2: ATC does not believe that 12 months is sufficient enough time for an entity to become compliant with all of the CIP standards. (CIP-003 – CIP-009) We believe that an 18 month window is needed for all Category 2 milestones. In addition, ATC believes that all of the standards should have the same milestone completion date. Although we agree that some Requirements can be done earlier we believe that having the same milestone window gives the entity the ability to put in place a more comprehensive implementation plan that aligns with bringing the Critical Asset into compliance. We don't believe that this reduces security but makes the implementation plan easier to manage and implement. The proposed timelines are problematic. If the electronic security perimeter and physical security need to be in place in 12 months, why is the training allowed to take 18 months? The training should be complete prior to implementing the changes. The varying timeline requirements add to the complexity of Milestone Category 2, which further supports making them all the same. Item 7a: Lastly, ATC believe that the SDT needs to move from a "month" counter to a "day" counter in Table 2. ATC is making this suggestion because an entity would be penalized with fewer days because its milestone month includes February. If the SDT disagrees with our suggestion, then we ask that they specify how many days are in a "month" and when does an entity start counting "months". When does the month counter start? Examples: An entity identifies a Critical Asset on the 1st day of a month. Does the counter start in the next month or does the month in which it was identified count? June 1st and entity identifies a new Critical Asset What is the milestone date for CIP-003 R4, R5 and R6? These requirements currently give an entity 6 months to reach compliance. A) December 31st or B) November 30th Would you give a different answer if the identification happens on June 30th? Additional information: FERC Docket RD09-7 states that the quarter in which something takes place is counted as part of the effective day counter. (See Footnote 8) In other words, FERC sees no difference between the June 1st and June 30th date, but in reality, compliance is either given an additional 30 days (June 1st) or loses 30 days (June 30th). ATC believes that this can be avoided if the team uses a day counter. (Calendar Days)
Group
Bonneville Power Administration
Denise Koehn
Yes
Yes
No
No

Group
Midwest ISO Standards Collaborators
Jason L. Marshall
Yes
Yes
Yes
While we agree that the SDT has addressed the concerns identified by the Commission in the FERC order, we do not believe the changes are closing a significant gap in reliability. At best, these changes simply expand upon the understanding of what the continuous escort requirement means. Thus, these changes do not warrant violating the Commission approved Reliability Standards Development Process by combining the commenting and pre-ballot review periods. The end result is that the Cyber Security - 706 Order standards drafting team has to divert their scarce resources from focusing on developing the next generation of the CIP standards to this fire drill exercise to make a small incremental improvement to the standard. There is no reason these changes could not have been addressed in the process of developing the next generation of CIP standards.
Yes
We agree that the modifications to the standards and implementation plans meet the intent of the FERC directives but do have some suggestions for improving them. 1) In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Category 1 Scenario under Newly Registered Entity Scenarios on page 8 appears to address what is largely a registration issue. It appears that the document assumes that the merging entities will join their registration but this may not be the case. There is no NERC rule that requires two utilities that operate separate balancing authorities to merge those balancing authorities once the merger is completed. They may continue to be registered as two BAs as a result. Consider the Duke-Cinergy merger as example of when this happened. The scenario should be updated to consider these issues or to identify the assumptions made. Further, we suggest the that the last two sentences in the second paragraph under the Category 1 Scenario beginning with following language should be deleted as a result: “it would be preferred that a single program be the result of this analysis, however,”. 2) In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, the first sentence (as shown below) in the second paragraph in section (a) under the Category 3 Scenario under Newly Registered Entity Scenarios should be deleted. That sentence is: “Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity’s risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets.” This sentence assumes that the primary purpose of the CIP standards is to protect the Critical Cyber Assets and that once a Critical Cyber Asset always a Critical Cyber Asset. Rather, the purpose is to protect the grid by ensuring it can’t be compromised by hacking of a cyber asset. It demonstrates ignorance that how the grid is operated can, will and should affect the Critical Asset list. Mergers can affect how the grid is operated and ultimately the Critical Asset list. As an example, a merged utility may combine its two previously separate Balancing Authorities into a single Balancing Authority. This would cause the Contingency Reserve obligation to increase and could cause a generating unit to be no longer a Critical Asset as a result. Table C-2 in NERC’s Security Guideline for the Electricity Sector: Identifying Critical Assets document specifically identifies a unit exceeding the Contingency Reserve obligation as a reason to classify a generating unit as a Critical Asset. This is hardly an extraordinary circumstance. Further, this outcome would occur even if the two merged entities had identical Critical Asset identification methodologies. 3) In an August 10, 2009 informational filing to FERC, NERC laid out a new approach to define one VRF at the requirement level that applies to the requirement and its sub-requirements and applies a single comprehensive set of VSLs to the main requirement that categorizes non-compliance with the main requirement and sub-requirement. This approach should be applied here. 4) The VRFs on CIP-006-3a R1.6 and R1.6.1 should be Lower because it is completely an administrative requirement intended to demonstrate to the Commission that visitors are escorted. Failure to have a visitor control program that includes logs is hardly a risk especially when one considers that other requirements such as CIP-006-3a R4 already mandate that a secure perimeter would be maintained. With R4 in place, a visitor could not gain unnecessary access even if there were no visitor log maintained. 5) For the VSLs on CIP-006-3a R1.6, a potential non-compliance that is likely to occur that is not considered is for the case of not logging egress when ingress is logged. VSLs could be written based on the number of visitors that don’t have egress logged. Likely, if ingress is not logged, egress will not be logged and no record of the visitor will exist. For this reason, the Moderate and High VSLs will likely never apply. The Moderate VSL appears to assume that the compliance auditor will be able to review a record of all visitors that were not

logged into the visitor log. The visitor log is intended to be the record of visitors so how will the compliance auditor know a visitor wasn't logged. No evidence would exist. 6) We suggest the following wording for CIP-006-3a R1.6.1 would be more succinct and provide the same meaning. "Visitor logs to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of the escort with authorized unescorted physical access performing the escort." 7) The drafting team should consider defining the term visitors in R1.6 and eliminating the clause in parentheses. Clauses like these could be misconstrued from its intention which is to define visitor. A definition is cleaner and clearer.

Consideration of Comments on Cyber Security Ninety-day Response — Project 2009-21

The Cyber Security Order 706 Standard Drafting Team thanks all commenters who submitted comments on the proposed revisions of CIP-002-2 through CIP-009-2, the Implementation Plan for Version 3 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, developed by the standard drafting team as part of Project 2009-21 Cyber Security Ninety-day Response. These standards were posted for a 30-day public comment period from October 13, 2009 through November 12, 2009. The respondents were asked to provide feedback on the standards through a special Electronic Comment Form. There were 29 sets of comments, including comments from more than 60 different people from approximately 40 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

The drafting team made the following changes following the initial comment period, prior to the initial ballot:

Changes to CIP-006-3

- In response to stakeholder comments the drafting team revised CIP-006-3 Requirement R1.6 as shown below to more closely address the specific directive included in the FERC Order approving Version 2 CIP Standards issued September 30, 2009.

  R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
  R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
  R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

Changes to Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

- Several stakeholders also asked for clarity on the following language that had been in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities concerning the date of first occurrence of a recurring requirement:

  > A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached.
  >
  > For those NERC Reliability Standard requirements that include a prescribed records retention period (e.g., retention of logs for 90 days), a Responsible Entity is expected to begin collection and retention of the required "data," "documents," "documentation," "logs," and "records" by the Compliant milestone date in Table 2.

For retention requirements that are triggered by a specific event (e.g., a reportable incident), collection and retention of the required "data," "documents," "documentation," "logs," and "records" begins with the triggering event. In this instance, the requirement for records collection and retention does not begin until the Compliant milestone date in Table 2 is reached and only applies to triggering events occurring after the Compliant milestone date.

The SDT acknowledged that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledged that this issue is not confined to the CIP standards alone and hence goes beyond the scope of this SDT. The drafting team removed the language from the implementation plan. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.

- The team also added language to clarify the meaning of the terms "compliant" and "auditably compliant" as used in the implementation plan, and added some language to clarify when to apply the "Category 1 Scenario" and "Category 2 Scenario" referenced in the plan, and changed some headings for improved clarity.

Changes to Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

- The drafting team modified the section of the plan that addressed retirement of earlier implementation plans to improve clarity.

The drafting team did not make any changes to the SAR, or to the proposed VRFs or VSLs that were posted for comment.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ralph Rufrano	New York Power Authority	NPCC	5
2.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
3.	Gregory Campoli	New York Independent System Operator	NPCC	2
4.	Roger Champagne	Hydro-Quebec TransEnergie	NPCC	2
5.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
6.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
7.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
8.	Brian D. Evans-Mongeon	Utility Services	NPCC	8
9.	Mike Garton	Dominion Resouces Services, Inc.	NPCC	5
10.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5
11.	Kathleen Goodman	ISO - New England	NPCC	2
12.	David Kiguel	Hydro One Networks Inc.	NPCC	1
13.	Michael R. Lombardi	Northeast Utilities	NPCC	1
14.	Randy MacDonald	New Brunswick System Operator	NPCC	2

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
15.	Greg Mason		Dynegy Generation	NPCC						5			
16.	Bruce Metruck		New York Power Authority	NPCC						6			
17.	Chris Orzel		FPL Energy/NextEra Energy	NPCC						5			
18.	Robert Pellegrini		The United Illuminating Company	NPCC						1			
19.	Saurabh Saksena		National Grid	NPCC						1			
20.	Michael Schiavone		National Grid	NPCC						1			
21.	Peter Yost		Consolidated Edison Co. of New York, Inc.	NPCC						3			
22.	Gerry Dunbar		Northeast Power Coordinating Council	NPCC						10			
23.	Lee Pedowicz		Northeast Power Coordinating Council	NPCC						10			
2.	Group	Ruth Blevins	Dominion Virginia Power	X		X		X					
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	john calder			SERC						1, 3			
2.	dennis sollars			SERC						1, 3, 5			
3.	paul rodi			SERC						5			
4.	randy reynolds			SERC						1			
5.	george wood			SERC						1			
3.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Doug Hohlbaugh		FirstEnergy	RFC						1, 3, 4, 5, 6			
2.	Dave Folk		FirstEnergy	RFC						1, 3, 4, 5, 6			
4.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Curt Wilkins		Transmission System Operations	WECC						1			
2.	Kelly Hazelton		Transmission System Operations	WECC						1			
5.	Group	Jason L. Marshall	Midwest ISO Standards Collaborators		X								

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	Additional Member	**Additional Organization**	**Region**						**Segment Selection**			
1.	Barb Kedrowski	We Energies	RFC						3, 4, 5			
2.	Michael Ayotte	ITC Holdings	RFC						1			
3.	Greg Rowland	Duke Energy	SERC						1, 3, 5, 6			
4.	Joe Knight	GRE	MRO						1, 3, 5			
5.	Eric Scott	Ameren	SERC						1			
6.	Bob Thomas	IMEA	SERC						4			
6.	Individual	Laurie Urbancik	Exelon									
7.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
8.	Individual	Ed Carmen	BGE CIP Core Team	X									
9.	Individual	Silvia Parada-Mitchell	Transmission Owner	X				X	X				
10.	Individual	Brent Ingebrigtson	E.ON U.S. LLC	X		X		X	X				
11.	Individual	Benjamin Church	NextEra Energy Resources					X					
12.	Individual	Jim Lauth	Silicon Valley Power			X	X	X					
13.	Individual	Jeremy Bergstrom	Navasota Odessa Energy Partners, LP					X					
14.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
15.	Individual	Michael Puscas	The United Illuminating Company	X		X							
16.	Individual	James Starling	South Carolina Electric and Gas	X		X		X	X				
17.	Individual	Steve Newman	MidAmerican Energy Company	X		X		X	X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Individual	Marty Berland	Progress Energy	X		X		X	X				
19.	Individual	Randy Schimka	San Diego Gas and Electric Co	X		X		X					
20.	Individual	James H. Sorrels, Jr.	American Electric Power	X		X		X	X				
21.	Individual	Patrick Brown	PJM Interconnection		X								
22.	Individual	Adam Menendez	Portland General Electric Company	X		X		X	X				
23.	Individual	Martin Bauer	US Bureau of Reclamation					X					
24.	Individual	Terrence Walsh	Consolidated Edison Company of New York INC.	X		X		X					
25.	Individual	Edward Bedder	Orange and Rockland Utilities Inc	X									
26.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
27.	Individual	Roger Champagne	Hydro-Québec TransEnergie (HQT)	X									
28.	Individual	Dan Rochester	Independent Electricity System Operator		X								
29.	Individual	Jason Shaver	American Transmission Company	X									

1. In its order approving CIP-002-2 through CIP-009-2, the Commission directed NERC to make changes to CIP-006-2 and CIP-008-2 as well as the implementation plan for newly identified critical cyber assets and file those changes within 90 days of the order. Do you agree that the SAR accurately addresses the scope of these directives? If not, please identify what you feel is missing in the SAR.

Summary Consideration:

About a quarter of the respondents provided comments on the SAR and its accurate representation of the FERC Order approving Version 2 CIP Standards issued September 30, 2009, which included direction to: add a requirement for a visitor control program (CIP-006); remove the statement regarding the removal of a component or system from service as part of the incident response plan test (CIP-008); and update the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

Many comments were positive that the SAR accurately reflected the Commission's directives. Concerns were raised regarding the impact of a visitor control program in CIP-006, especially with field operations, requiring visitors to sign in and out every time a physical security perimeter is crossed, and be escorted. These issues were clarified by the SDT in its responses.

Other comments applauded the SDT for following the standard development process and preparing a compliance filing in an extremely shortened timeframe.

The current revisions to the CIP-006 and CIP-008 standards and the implementation plans were given a very high priority by FERC. In response, the Cyber Security Order 706 standard drafting team re-organized its resources and schedule, and together with the industry, made the effort to incorporate the directed changes while following the NERC standard development process in a compressed timeframe.

The SDT made the following modification to the CIP standards, based on stakeholder comments:

Revised the CIP-006 R1.6 requirement as shown below to more closely address the specific directives included in the FERC Order approving Version 2 CIP Standards issued September 30, 2009.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

Organization	Yes or No	Question 1 Comment
NextEra Energy Resources	No	Generally we agree with the proposed changes. However, one area of concern is CIP-006-2. We feel that it should not be a requirement for persons with unescorted physical access to have to swipe out when leaving the PSP. Swiping in should be sufficient.
Response: The SDT clarifies that Requirement CIP-006 R1.6 specifies a visitor control program. The SDT did not modify the requirements for individuals with authorized unescorted access to the Physical Security Perimeter. CIP-006 R6 requires a log that captures "time of access" for all individuals who enter a Physical Security Perimeter. Project 2008-15 "Interpretation of CIP-006-1a By US Army Corps of Engineers" clarifies that the term "time of access" indeed refers to the time an authorized individual enters the physical security perimeter.		
Florida Power & Light	No	Generally we agree with the proposed changes. However, one area of concern is CIP-006-2. We feel that it should not be a requirement for persons with unescorted physical access to have to swipe out when leaving the PSP. Swiping in should be sufficient.
Response: The SDT clarifies that Requirement CIP-006 R1.6 specifies a visitor control program. The SDT did not modify the requirements for individuals with authorized unescorted access to the Physical Security Perimeter. CIP-006 R6 requires a log that captures "time of access" for all individuals who enter a Physical Security Perimeter. Project 2008-15 "Interpretation of CIP-006-1a By US Army Corps of Engineers" clarifies that the term "time of access" indeed refers to the time an authorized individual enters the physical security perimeter.		
Portland General Electric Company	No	
American Transmission Company	Yes	ATC agrees that the SAR reflects the Commission's directive but we do not agree with all of the proposed changes. (Please see our specific comments in the other questions.)
Response: Thank you for your comments		
US Bureau of Reclamation	Yes	We applaud the SDT in following the standards development process by submitting an implementaton plan that addresses the Commissions order. This is consistent with the Commissions requirement that "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order" it is also consistent with the process for submitting revision (Reference 16 USC Sec. 824o (d) (5) The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.)

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments		
FirstEnergy	Yes	We commend NERC for their expedient response to FERC's directives.
Response: Thank you for your comments		
San Diego Gas and Electric Co	Yes	While the SAR does accurately address the scope of the FERC directives, we would suggest that the SAR's name be changed to something more descriptive than "Cyber Security Ninety-Day Response" to make it easier to locate and understand in the future. Perhaps a SAR title like "NERC response to FERC Cyber Security V2 Std Approval" would help to make the contents clearer when searching or browsing in the future.
Response: Thank you for your comments. We will submit the suggestion for future Project Naming.		
American Electric Power	Yes	
BGE CIP Core Team	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York INC.	Yes	
Dominion Virginia Power	Yes	
Duke Energy	Yes	
E.ON U.S. LLC	Yes	
Exelon	Yes	
Hydro-Québec TransEnergie (HQT)	Yes	
Independent Electricity System	Yes	

Organization	Yes or No	Question 1 Comment
Operator		
Manitoba Hydro	Yes	
MidAmerican Energy Company	Yes	
Midwest ISO Standards Collaborators	Yes	
Navasota Odessa Energy Partners, LP	Yes	
Northeast Power Coordinating Council	Yes	
Orange and Rockland Utilities Inc	Yes	
PacifiCorp	Yes	
PJM Interconnection	Yes	
Silicon Valley Power	Yes	
South Carolina Electric and Gas	Yes	
The United Illuminating Company	Yes	

2. Do you agree that the proposed modifications to CIP-006-2, CIP-008-2, and the implementation plans meet the intent of the Commission's directives? If not, please identify what changes you feel are needed to meet the intent of these directives.

Summary Consideration:

About half of the respondents provided feedback regarding the proposed modifications to CIP-006, CIP-008, and the Implementation Plans to meet the intent of the Commission's directives. The majority of the issues that were raised concerned the requirements associated with the visitor control program and the Implementation Plan requirements. The commenters suggested that the visitor control program requirements stated in CIP-006 may have gone beyond the directive from FERC in its Order approving Version 2 CIP Standards issued September 30, 2009 by requiring the documentation of visitor identity, purpose of visit, time and date of entry and exit from physical security perimeters, and the identity of the escort since this may go beyond the readily available technology of badging systems, especially in field locations.

Many commenters were concerned that the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities includes language stating that the first occurrence of a recurring requirement must be completed by the Compliant milestone date. Others were looking for guidance on the treatment of newly acquired assets if acquired from a third party.

These requirements were clarified by the SDT in its responses. The comments on the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities were considered by the SDT and determined to be more of a compliance issue that would be more appropriately addressed by NERC Compliance staff. The language concerning the required date of compliance in the Implementation Plan was removed and the issue referred.

The SDT made the following modification to the standard, based on stakeholder comments:

- Revised the language in CIP-006 R1.6 to not be overly prescriptive in defining the requirements for the visitor control program. (See the Summary Consideration for question 1 for the specific changes.)
- Removed the following language from the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities concerning the date of first occurrence of a recurring requirement – the NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue:

> A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached.

For those NERC Reliability Standard requirements that include a prescribed records retention period (e.g., retention of logs for 90 days), a Responsible Entity is expected to begin collection and retention of the required "data," "documents," "documentation," "logs," and "records" by the Compliant milestone date in Table 2.

For retention requirements that are triggered by a specific event (e.g., a reportable incident), collection and retention of the required "data," "documents," "documentation," "logs," and "records" begins with the triggering event. In this instance, the requirement for records collection and retention does not begin until the Compliant milestone date in Table 2 is reached and only applies to triggering events occurring after the Compliant milestone date.

For those NERC Reliability Standard requirements that do not include a specified periodicity or records retention requirement, a Responsible Entity is expected to have available all records required to demonstrate compliance to these requirements by the Compliant milestone date in Table 2.

Organization	Yes or No	Question 2 Comment
Consolidated Edison Company of New York INC.	No	CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – "Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor." We suggest: "R1.6.1. Visitor logs (manual or automated) to identify visitors, the purpose of the visit, the date and time of entry and exit from the Physical Security Perimeters, and to identify personnel with authorized, unescorted physical access performing the escort." CIP-006 R1.6.2 should be modified to "R1.6.2. Requirement for continuous escorted access of visitors within the Physical Security Perimeter." The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For more information see the answer to question 4.

Response:

CIP-006 R1.6.1:

The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.

The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in

Organization	Yes or No	Question 2 Comment
implementing a more rigorous visitor log if they so choose. **CIP-006 R1.6.2:** **The SDT agrees that the modification to CIP-006 R1.6.2 adds clarity and does not modify the intent. CIP-006 R1.6.2 has been modified as suggested.** **Implementation Plan:** **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Hydro-Québec TransEnergie (HQT) Independent Electricity System Operator Northeast Power Coordinating Council	No	CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – "Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor." CIP-006 R1.6.2 should be modified to "Requirement for continuous escorted access of visitors within the Physical Security Perimeter." The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For additional information see the response to question 4.
Response: **CIP-006 R1.6.1:** **The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.** **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.**		

Organization	Yes or No	Question 2 Comment
CIP-006 R1.6.2: **The SDT agrees that the modification to CIP-006 R1.6.2 adds clarity and does not modify the intent. CIP-006 R1.6.2 has been modified as suggested.** **Implementation Plan:** **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Orange and Rockland Utilities Inc	No	CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination - Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor. We suggest: R1.6.1. Visitor logs (manual or automated) to identify visitors, the purpose of the visit, the date and time of entry and exit from the Physical Security Perimeters, and to identify personnel with authorized, unescorted physical access performing the escort. CIP-006 R1.6.2 should be modified to R1.6.2. Requirement for continuous escorted access of visitors within the Physical Security Perimeter. The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For more information see the answer to question 4.
Response: **The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the**		

Organization	Yes or No	Question 2 Comment
use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive. **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.** **CIP-006 R1.6.2:** **The SDT agrees that the modification to CIP-006 R1.6.2 adds clarity and does not modify the intent. CIP-006 R1.6.2 has been modified as suggested.** **Implementation Plan:** **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
San Diego Gas and Electric Co	No	CIP-008-2: We are in agreement with the proposed modifications to CIP-008-2. CIP-006-2: In the modifications made to CIP-006-2, we have an issue with the language requiring the documentation of "entry to and exit from Physical Security Perimeters." Many badging systems document personnel ingress to PSP areas, but not egress and some entities may utilize their badging system to track visitors (visitors swipe for record keeping purposes but their badge cannot open any access points). A recent interpretation of CIP-006 also confirmed that only ingress monitoring is required, and that is the functionality delivered by many badge access systems. After their visit is completed, a visitor typically signs out at the central Security Station and surrender their visitor badge at that time. In order to make the R1.6 language more easily understood, our first preference would be to remove the "and exit from" language. If that cannot be done, then our second preference would be to change the language in R1.6.1 to "date of entry to and last exit of the day from Physical Security Perimeters". Manually logging all visitor ingress and egress from CCA areas could be potentially very time-consuming without providing additional reliability to the Bulk Electric System. Implementation Plans:

Organization	Yes or No	Question 2 Comment
		In the Implementation plan language, we were looking for particular guidance showing how an asset would be treated if acquired from a third party. In particular, there could be a scenario where the current owner does not list any critical assets or critical cyber assets. Once the acquisition takes place, what accommodations should be made in the implementation plan if the new owner feels that there are critical assets or critical cyber assets associated with the asset? It could theoretically take a considerable amount of time to start a proper Cyber Security program for the acquired plant from scratch. A 12 month implementation plan schedule may not be practical given the complexity of assessing the acquired plant and making the necessary cyber security modifications and additions for Compliance. We'd like to suggest that a 24 month implementation plan schedule would be more appropriate in cases like this.

Response:

CIP-008-2:

Thank you for your comment

CIP-006-2:

The SDT does not agree that the requirement forces a very time-consuming process on the entity in logging the ingress and egress of visitors from Physical Security Perimeters. It is the opinion of the SDT that documenting precisely when unauthorized individuals had escorted access inside Physical Security Perimeters is a key element of a strong visitor control program. The SDT reminds the entity that it also has the discretion to grant an individual authorized unescorted physical access to the Physical Security Perimeter should the requirement of escorting and logging ingress and egress prove burdensome.

Implementation Plan:

- **Where the third party did not identify this asset as a critical asset and did not have a CIP compliance program in place for the acquired asset, if the current owner does not list any critical assets or critical cyber assets, and as a result of the acquisition of the asset, it has one year from the date of the acquisition to merge the CIP programs and conduct its risk-based methodology, or at the required one year review of its application of the CIP-002 Critical Asset risk-based methodology since the last application, whichever is earlier. The scenario indicates that the application of the methodology now determines that this is a newly identified Critical Asset. Under the Implementation Plan, the newly identified Critical Asset's implementation of the CIP program falls under category 1 and the entity has 24 months from the date of the identification of the Critical Asset with Critical Cyber Assets to implement its CIP program for these Critical Cyber Assets, as per the Category 1 column of Table 2. This is explained in the Newly Registered Entity Scenario 1 (Application of Category 1 of the Implementation Plan, "A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset," Page 8.**

- **Where the third party has identified the acquired asset as a Critical Asset containing Critical Cyber Assets prior to the acquisition and therefore had a CIP program for these cyber assets, the CIP program can independently be operated and the entity has one year to decide whether to merge the programs under a single Senior Manager. In either case, the CIP program is already effective and applicable upon**

Organization	Yes or No	Question 2 Comment
acquisition. This is explained under Newly Registered Entity Scenario 1 (Application of Category 2, "A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset," Page 9.		
E.ON U.S. LLC	No	In paragraph 29 of the Order, the Commission approves version 2 of the standard on the basis that continuous is analogous to supervised. Furthermore, the Commission states as its goal that Responsible Entities implement visitor control programs and be able to reasonably demonstrate that they maintain such programs. The order reiterates that the Version 2 standards achieve this goal. The proposed changes to CIP-006-2 do not meet the Commission's goal because of prescriptive measures that do not allow for reasonable demonstration
Response: The modifications to CIP-006 were made in direct response to paragraph 30 of the FERC Order approving the Version 2 CIP Standards issued September 30, 2009. Respectfully, the SDT does not agree that the requirement to implement a visitor control program is overly prescriptive or that it cannot be reasonably demonstrated. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).		
NextEra Energy Resources Silvia Parada-Mitchell Florida Power & Light	No	In reading the second sentence of the New Asset Implementation Plan redline which starts, "In those instances?" it seems that this is stating that an entity must demonstrate compliance prior to the actual Compliant date set forth in the current implementation plan. The implementation plan right now states that the period of time between the Compliant date and Auditably Compliant date is when you must start keeping records, logs, documents, etc. If the current proposal goes through, the entity would need to conduct its first vulnerability assessment sometime prior to the Compliant date. This is a huge shift and shortens the implementation window up to a year. Hence, we feel this change should not be approved.
Response: Thank you for your comment **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Manitoba Hydro	No	The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was modified beyond the Commision's directives in RD09-7-000. See response to Question 4.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The Standards Drafting Team has responded to your comments in its response to Question 4, below.		
Exelon	No	We do not agree with the CIP-006-3 R1.6 change where you have included the requirement for the visitor log to contain "...the identity of personnel with authorized, unescorted physical access performing the escort." This would be an excessive administrative burden that goes beyond what FERC ordered in paragraph 30 which simply stated "...the commission directs the ERO to develop a modification to Reliability Standard CIP-006-2, through the NERC Reliability Standards development process, to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit, within 90 days of the date of this order". Your additional requirement can be interpreted to mean any hand off of escort responsibilities would also need to be documented which would be an excessive administrative burden that would provide no additional assurances or security. An acceptable alternative would be for the visitor log to include a reference to the site contact and reason for the visit. These are things known at the time of visitor sign in which would not require additional updates through out the time the visitor remains within the secure area.
Response: CIP-006 R1.6.1: **The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.** **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.**		
Portland General Electric Company	No	
American Transmission Company	Yes	ATC does not agree with the deletion of the following sentence from CIP-008-2 R1.6 “Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test”. Although, ATC believes that FERC is correct in its assessment that the sentence could be inferred by Requirement 1 and Requirement 1.6, it does not harm the requirement in any way by remaining part of the standard and should not be deleted. The Commission goes as far as to say that the sentence is similar to an interpretation, so, if that is the case, we don’t see any harm in keeping it as part of the standard. Lastly, ATC is concerned that we could be back to this same spot if an entity requests a formal definition of this requirement. From the SDT perspective, what issues are being addressed by removing this sentence? Does the SDT believe that the deletion of this specific sentence will not require the removal of equipment in order to be in compliance with the standard? ATC believes that the sentence does provide additional clarity of the requirements and does not harm reliability and, therefore, should not be removed from the standard. As the Commission clearly points out, this sentence does provide an interpretation or clarification of the standard

Organization	Yes or No	Question 2 Comment
		which the Commission did not disagree. If the SDT does remove this sentence, then we request the SDT to identify any concerns or issues with the interpretation or clarification. (Deleted Sentence) Specifically, would the SDT give an alternate interpretation of this requirement?
Response: In response to the FERC Order 706, the SDT understood that FERC had provided direction in par. 687, "the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise", which required the inclusion of the statement. Subsequently, in the FERC Order approving the Version 2 CIP Standards issued September 30, 2009, the Commission directed NERC to remove this statement and stated in their determination that "we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement". **This statement was additional information, not a requirement, whose inclusion or removal from the standard does not affect the implementation of the requirement, and can be removed. The language of the requirement does not require removal of equipment from service. This information could be included in future guidance documentation. The SDT is not aware of any issues with this clarification.**		
South Carolina Electric and Gas	Yes	Order No. 706-B Nuclear Implementation schedule should be added to the implementation table for the proposed modifications to CIP-006-2, CIP-008-2 in order to avoid any confusion between the two schedules.
Response: The Version 2 and Version 3 CIP Standards implementation is independent of the 706B implementation plan. Specifically, the Version 2 implementation date is 4/1/10. The first milestone under the 706B implementation plan is 12 months following FERC approval, which is after 4/1/10, and likely into 2011.		
American Electric Power	Yes	
BGE CIP Core Team	Yes	
Bonneville Power Administration	Yes	
Dominion Virginia Power	Yes	
Duke Energy	Yes	
FirstEnergy	Yes	

Organization	Yes or No	Question 2 Comment
MidAmerican Energy Company	Yes	
Midwest ISO Standards Collaborators	Yes	
Navasota Odessa Energy Partners, LP	Yes	
PacifiCorp	Yes	
PJM Interconnection	Yes	
Silicon Valley Power	Yes	
The United Illuminating Company	Yes	
US Bureau of Reclamation	Yes	

3. Do you have any additional comments associated with the proposed SAR for Project 2009-21: Cyber Security Ninety-day Response? If yes, please explain.

Summary Consideration:

About a third of the respondents provided additional comments and feedback concerning the proposed SAR for Project 2009-21: Cyber Security Ninety-day Response. A number of comments addressed the respondents' concern of not following the approved SAR process in the development and implementation of this SAR. The concerns were related to the potential for introduction of ambiguity and not having the time to openly discuss the issues that the SAR is addressing. The perception was that the imposition of an unreasonably short schedule threatens to undermine the standards development process being followed by NERC.

Organization	Yes or No	Question 3 Comment
American Electric Power	No	
American Transmission Company	No	
BGE CIP Core Team	No	
Bonneville Power Administration	No	
Dominion Virginia Power	No	
Duke Energy	No	
E.ON U.S. LLC	No	
Exelon	No	
Manitoba Hydro	No	
MidAmerican Energy Company	No	

Organization	Yes or No	Question 3 Comment
Navasota Odessa Energy Partners, LP	No	
PJM Interconnection	No	
Portland General Electric Company	No	
Progress Energy	No	
San Diego Gas and Electric Co	No	
Silicon Valley Power	No	
South Carolina Electric and Gas	No	
The United Illuminating Company	No	
US Bureau of Reclamation	No	
NextEra Energy Resources Florida Power & Light	Yes	Although the SAR proposes many changes, these changes lead to ambiguity and this ambiguity lends more latitude to the regions.
Response: Thank you for your comment. The changes proposed in the SAR were in response to the FERC directive.		
PacifiCorp	Yes	Comments: PacifiCorp generally supports the Request for Rehearing or Clarification submitted by the Edison Electric Institute (EEI) submitted in FERC Docket No. RD09-7 on October 30, 2009. Specifically, PacifiCorp agrees with EEI that the ninety-day deadline imposed by FERC's September 30, 2009 to modify the CIP Reliability Standards is unreasonably short. In addition, PacifiCorp is concerned that this type of unreasonable deadline threatens to undermine NERC's standards development process. Currently, the NERC standards development process is the only opportunity for industry stakeholders to participate in the development of reliability standards that will have significant operational and business impacts. Unreasonable deadlines set by FERC and the corresponding "expedited" standards development process threatens to undermine the robustness of the current process. While PacifiCorp does not have substantive issues with the current proposed changes, it is concerned regarding the procedure being used here to adopt

Organization	Yes or No	Question 3 Comment
		these changes.
Response: The drafting team asked the Standards Committee to approve use of the "Urgent Action" standard development process so that the team could address the directives without requesting a variance from the standards process. Under the "Urgent Action" process, a SAR and proposed standard (and implementation plan) are all posted at once for a 30-day pre-ballot review, followed by the initial ballot. The Standards Committee directed the drafting team to post the SAR and proposed standard for a 30-day comment period, followed as quickly as practical by the initial ballot. In making this decision, the Standards Committee was attempting to provide respondents with an opportunity to provide comment on the proposed modifications before proceeding to ballot. Posting a SAR with a proposed standard is not a violation of the standards development process – this is allowed. The Standards Committee reports to the NERC Board of Trustees and has dual obligations – to protect the integrity of the standards process and to assist NERC in meeting its obligations as the ERO.		
Consolidated Edison Company of New York INC. Hydro-Québec TransEnergie (HQT) Independent Electricity System Operator Northeast Power Coordinating Council	Yes	Development of this SAR should follow the approved SAR process
Response: The drafting team asked the Standards Committee to approve use of the "Urgent Action" standard development process so that the team could address the directives without requesting a variance from the standards process. Under the "Urgent Action" process, a SAR and proposed standard (and implementation plan) are all posted at once for a 30-day pre-ballot review, followed by the initial ballot. The Standards Committee directed the drafting team to post the SAR and proposed standard for a 30-day comment period, followed as quickly as practical by the initial ballot. In making this decision, the Standards Committee was attempting to provide respondents with an opportunity to provide comment on the proposed modifications before proceeding to ballot. Posting a SAR with a proposed standard is not a violation of the standards development process – this is allowed. The Standards Committee reports to the NERC Board of Trustees and has dual obligations – to protect the integrity of the standards process and to assist NERC in meeting its obligations as the ERO.		
FirstEnergy	Yes	We understand that NERC is merely responding to directives with a specific completion time frame of 90-days. And we believe that NERC has done this job well. Unfortunately, due to the short 90-day time frame, NERC and its stakeholders did not have much time to challenge FERC's directives. We offer the following as strictly comments on the directive to modify CIP-008: CIP-008 Req. R1.6

Organization	Yes or No	Question 3 Comment
		FERC feels that the statement "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test" should be removed and NERC has proposed to remove it per the directive by FERC. It is interesting to note that in Order 706 par. 687, FERC stated "the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise" Yet, in the recent Order, per par. 38, FERC has directed NERC to remove this statement and stated in their determination "we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement". It appears that FERC may have inadvertently sent unclear and inconsistent messages when it said "the ERO should clarify" in Order 706, and then asked NERC to remove the statement in the recent Order because it is merely a "clarification of the requirement". It is not clear how removing this statement makes R1.6 a better requirement since, as FERC says, "...it is similar to an interpretation or clarification of a requirement." In addition, the phrase, "A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise..." is also a clarifying statement and the FERC raised no concern over its inclusion in this standard requirement. The direction to remove clarifying statements seems to go against the goal of writing clear and concise reliability standards.
Response: In response to the FERC Order 706, the SDT understood that FERC had provided direction in par. 687, "the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise", which required the inclusion of the statement. Subsequently, in the FERC Order approving the Version 2 CIP Standards issued September 30, 2009, the Commission directed NERC to remove this statement and stated in their determination that "we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement". **This statement was additional information, not a requirement, whose inclusion or removal from the standard does not affect the implementation of the requirement, and can be removed. The language of the requirement does not require removal of equipment from service. This information could be included in future guidance documentation. The SDT is not aware of any issues with this clarification.**		
Midwest ISO Standards Collaborators	Yes	While we agree that the SDT has addressed the concerns identified by the Commission in the FERC order, we do not believe the changes are closing a significant gap in reliability. At best, these changes simply expand upon the understanding of what the continuous escort requirement means. Thus, these changes do not warrant violating the Commission approved Reliability Standards Development Process by combining the commenting and pre-ballot review periods. The end result is that the Cyber Security - 706 Order standards drafting team has to divert their scarce resources from focusing on developing the next generation of the CIP

Organization	Yes or No	Question 3 Comment
		standards to this fire drill exercise to make a small incremental improvement to the standard. There is no reason these changes could not have been addressed in the process of developing the next generation of CIP standards.
Response: The SDT understands and appreciates your concerns, but issues regarding FERC's imposed timeline cannot be addressed in response to comments.		
Orange and Rockland Utilities Inc	Yes	

4. Do you have any additional comments associated with the proposed CIP-006-2, CIP-008-2, and the implementation plans? If yes, please explain.

Summary Consideration:

Nearly all of the respondents provided comments to the proposed CIP-006-2, CIP-008-2, and Implementation Plan Requirements. The majority of the issues that were raised concerned the respondents' need for a better understanding of the Implementation Plan requirements.

Many comments referred to the language concerning the start date for demonstration of compliance with recurring requirements. Other significant comments addressed the prescriptive nature of the requirements for the visitor control program and the treatment of combined assets from merged or acquired Registered Entities.

The SDT made no additional modifications to the standards and implementation plan requirements, based on these respondent comments.

Organization	Yes or No	Question 4 Comment
Exelon	No	1) For the "Implementation Plan for "Newly Registered Entities", we suggest the that the last two sentences in the second paragraph under the Category 1 Scenario beginning with following language should be deleted: "it would be preferred that a single program be the result of this analysis, however". 2) For the "Implementation Plan for "Newly Registered Entities", we suggest that the last two sentences of the Scenario 3, (a) paragraph be deleted: "It would be preferred that a single program be the result of this analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002."
Response: Thank you for your comments **1) This statement in the Implementation Plan is not a requirement. The statement is intended to provide guidance. It is the opinion of the SDT that a single program reduces complexity for both the Responsible Entity and the compliance monitoring and enforcing organizations.** **2) This statement in the Implementation Plan is not a requirement. The statement is intended to provide guidance. It is the opinion of the SDT that a single program reduces complexity for both the Responsible Entity and the compliance monitoring and enforcing organizations. Further, it reinforces that "Registered Entity specific circumstances may dictate or allow the two programs to continue separately."**		
American Electric Power	No	
Bonneville Power Administration	No	

Organization	Yes or No	Question 4 Comment
Navasota Odessa Energy Partners, LP	No	
San Diego Gas and Electric Co	No	
South Carolina Electric and Gas	No	
The United Illuminating Company	No	
US Bureau of Reclamation	No	
BGE CIP Core Team	Yes	1. Clarification is needed on how to apply a visitor control program for PSPs that have been established at a cabinet level (e.g., CCAs, or equipment treated as a CCA per CIP requirements, are housed within a secured cabinet that is located within a data center, and they are the only CCAs within the data center. Access to the cabinet that houses the CCAs is controlled, and therefore the cabinet serves as the PSP for these cyber assets)? 2. What is the implementation plan for the CIP Version 3 Reliability Standards?
Response: **1) The SDT leaves the specific details of interpreting the standards to their unique environment up to the entity.** **2) The "Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3" says that "The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard". Under Proposed Effective Date, end of Page 1, the current Proposed Effective Date in each standard for Version 3 specifies: "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)."**		
FirstEnergy	Yes	CIP-007 Per NERC Project 2009-16, the stakeholders and NERC's Board recently approved an interpretation of Req. R2 to clarify that the meaning of ports in this requirement is referring to "logical" ports. NERC may want to consider adding this interpretation to CIP-007 Version 3 so that it gets incorporated into the standard expediently rather than wait until a later time. Waiting until a later time will require both another revision to the standard and an extra filing by NERC to add the interpretation.
Response: The drafting team limited its modifications to CIP-007 to just those conforming changes needed for accuracy in identifying associated standards - no changes were made to any of the requirements in this set of standards to incorporate interpretations. The interpretation of CIP-007 for		

Organization	Yes or No	Question 4 Comment
WECC was approved by the BOT on November 5, 2009 and has not been filed for regulatory approvals. Interpretations do not become effective until approved by regulatory authorities. **Note that the interpretation becomes linked to the standard it clarified - and in this case will need to be carried forward and attached to later versions of the same standard if the requirement remains the same in each version.**		
PJM Interconnection	Yes	Comments: PJM would like to request clarification on the meaning of "identity" in CIP 006-3, Requirement R1.6.1; "Visitor logs to document visitor's identity, time and date of..." It is not clear, if the logs should only contain the visitor's name or it should require some form of verification of his/her identity, such as, a government (federal or local) issue photo ID. PJM is in agreement with a "Medium" VRF for standard number "CIP-006-3a", Requirement number "R1.6.1", if the clarification of "identity" represents the verification of the individuals identity; however, if the clarification of "identity" means, that the log should only contain "name only", PJM suggest the VRF of "Low".
Response: **The SDT agrees that there was some confusion around this issue and has modified the standard requirement to more closely align with the FERC order. See the summary consideration in response to question 1 to see how R1.6.1 was changed. (Page 7 of this report)** **It is the opinion of the SDT that 'facilities security' is critically important, as also indicated by the Commission, and that visitor control programs and visitor logs are an essential element of sound facilities security. Therefore, it is the opinion of the SDT that a VRF of "Medium" is appropriate for R1.6.1.**		
American Transmission Company	Yes	Implementation Plan Comments: Item 1: What does the word "compliant" mean when used in the phrase "when Registered Entities has been required to be compliant with NERC Reliability Standard CIP-002"? Does the team mean the "compliant" phase identified in the Original CIP Implementation plan? or, Does the team mean when an entity had to be either "substantially compliant" or "auditable compliant"? The Version 1 Implementation plan identifies three compliant phases. Substantially Compliant, Compliant, and Auditably Compliant. Item 2: Question about the last paragraph on page 3: (For example, if a particular transmission substation has been designated??)This example is structured around the premise that an entity has identified a Critical Asset but has not identified any associated Critical Cyber Asset and seems to point to scenario 3. Is this an example for scenario 3? If so, the SDT should insert an affirmative sentence linking it to scenario 3. Item 3:Question about paragraph 2 on page 4: (If, however, a particular transmission substation with Cyber Assets does not) What scenario (1, 2 or 3) is this paragraph attempting to address? It seems that it may be

Organization	Yes or No	Question 4 Comment
		attempting to provide an example of scenario 2 and, if so, we would suggest that the SDT provide a specific sentence linking it to a specific scenario. Item 4:Comment on Figure 1: (Category Selection Process Flow)ATC is concerned that the flow chart is assigning a new requirement for CIP-002-2 requirement 1. Based on the proposed flow chart, it seems that an entity has to determine prior to commissioning, any planned changes that would place a facility on an entity's Critical Asset list. We believe that the flow chart should be modified to state that a planned change to a known Critical Asset has to be Compliant upon commissioning and that a planned change which causes an existing facility to be placed on the Critical Asset list be allowed to follow Category 2. This additional clarity would address our concern of pre-determination of a Critical Asset for all planned changes. Would an entity be non-compliant if following a completion of planned change the entity subsequently determines that the facility is a Critical Asset? We are asking this question because the flow chart seems to be indicating that entities have to determine Critical Asset prior to commissioning, and if they determined later that a facility is a Critical Asset that entity could be found non-compliant. ATC suggest the following changes: Clarify that for existing Critical Assets any changes to its associated Critical Cyber Assets shall be compliant upon commissioning. Any newly identified Critical Assets will have to follow Category 2 for its associated Critical Cyber Assets. We believe that this change would accurately align with the existing CIP standards. Comments on the Category X (1, 2 and 3) Scenarios: (Page 6 and 7)The SDT has identified three Scenarios a) Category 1 Scenario, b) Category 2 Scenario, and c) Compliant upon Commissioning. Are these scenarios meant to be examples or does the SDT intend on these being specific scenarios meant to define Figure 1 Item 5: Second paragraph page 10: ("Registered Entities are encouraged when combining separate risk-based"?) ATC believes that the proposed Implementation plan needs to contain a qualifying statement that the annual application of an entities risk-based assessment methodology allows for the addition or removal of Critical Assets. Standard CIP-002 allows an entity to update its list based on the application of the risk-based assessment methodology and does not require a demonstration of "extraordinary circumstances" for removing a previously identified Critical Asset from its list. We believe that this statement is inserting additional compliance obligations that are not contained within the standard. Suggested Modification: Delete the first sentence. If the SDT does not agree with our suggestion, they need to indicate the language contained within CIP-002 which supports the inclusion of phrase "demonstrate extraordinary circumstances" within the standard. Item 6:Table 1: ATC does not believe that enough clarity exists between the phrase Existing Asset and Planned modification. Is a company non-compliance with CIP-002 if a planned modification becomes a Critical Asset following commissioning? (Example: An upgrade is made to an existing asset and it was not identified previously as a Critical Asset. Following commissioning: During the annual application of an entity's

Organization	Yes or No	Question 4 Comment
		risk-based assessment methodology the new asset is identified as a Critical Asset. Does category 2 apply?) Item 7:Table 2: ATC does not believe that 12 months is sufficient enough time for an entity to become compliant with all of the CIP standards. (CIP-003 - CIP-009) We believe that an 18 month window is needed for all Category 2 milestones. In addition, ATC believes that all of the standards should have the same milestone completion date. Although we agree that some Requirements can be done earlier we believe that having the same milestone window gives the entity the ability to put in place a more comprehensive implementation plan that aligns with bringing the Critical Asset into compliance. We don't believe that this reduces security but makes the implementation plan easier to manage and implement. The proposed timelines are problematic. If the electronic security perimeter and physical security need to be in place in 12 months, why is the training allowed to take 18 months? The training should be complete prior to implementing the changes. The varying timeline requirements add to the complexity of Milestone Category 2, which further supports making them all the same. Item 7a:Lastly, ATC believe that the SDT needs to move from a "month" counter to a "day" counter in Table 2. ATC is making this suggestion because an entity would be penalized with fewer days because its milestone month includes February. If the SDT disagrees with our suggestion, then we ask that they specify how many days are in a "month" and when does an entity start counting "months". When does the month counter start? Examples: An entity identifies a Critical Asset on the 1st day of a month. Does the counter start in the next month or does the month in which it was identified count? June 1st and entity identifies a new Critical Asset What is the milestone date for CIP-003 R4, R5 and R6? These requirements currently give an entity 6 months to reach compliance. A) December 31st or B) November 30th Would you give a different answer if the identification happens on June 30th? Additional information: FERC Docket RD09-7 states that the quarter in which something takes place is counted as part of the effective day counter. (See Footnote 8) In other words, FERC sees no difference between the June 1st and June 30th date, but in reality, compliance is either given an additional 30 days (June 1st) or loses 30 days (June 30th). ATC believes that this can be avoided if the team uses a day counter. (Calendar Days)

Response:

Item 1: The term Compliant is defined in the Version 1 Implementation Plan. This definition will be included in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

Item 2: Newly Registered Entity Scenario 1 (Application of Category 3 deals with "A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset", and does not address cases where new cyber assets are

Organization	Yes or No	Question 4 Comment
commissioned in an existing Critical Asset. The Standards Drafting Team assumes you mean Newly Registered Entity Scenario 1 (Application of Category 3 and has added additional clarification in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. **Item 3: This could apply to Category 1 or 2 scenarios. Additional clarification has been included in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.** **Item 4: The flow chart is a simplified flow for illustration and is not intended to cover all possible scenarios. A more detailed description of the Categories follows the flow chart. It is the opinion of the SDT that the combination of the flow chart, the detailed descriptions and the scenarios present an accurate and comprehensive treatment of the application of the categories and the implementation tables.** **Item 5: It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of risk-based methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.** **Item 6: It is the opinion of the SDT that the Implementation Plan, when considered in totality, is clear on a newly identified Critical Asset. Category 1 or Category 2 applies depending on whether the Responsible Entity has an existing CIP Program covering existing Critical Cyber Assets or not.** **Item 7: The Category 2 milestones have been simplified by using 6 month increments. It is the opinion of the SDT that the 6 month increments reflects adequately the graduated complexity of the requirements. In reference to the question about the 12 months for the implementation of electronic security perimeters and physical security perimeters, it is the opinion of the SDT that 6 months provides enough time for entities to complete the training of the personnel identified as a result of the implementation of the electronic and physical security perimeters.** **Item 7a: It is the opinion of the SDT that the month counter begins the first day of the month following a triggering event.**		
MidAmerican Energy Company	Yes	Implementation plan for Newly Identified Critical Cyber Assets: MidAmerican appreciates the specificity in the implementation plan for newly identified Critical Cyber Assets, identified under table 2. Four paragraphs (periodicity or recurrence of the requirement activity, prescribed record retention periods, specific event triggered requirements and records to demonstrate compliance when there is no specified periodicity) provide clarification. Newly Registered Entity Scenarios, Scenario 3a: When combining separate risk-based methodologies, a methodology that provides the most robust level of protection against a cyber attack should be selected. The resulting methodology should be applied to the combined system with no requirement that the resultant list contain all of the critical assets previously identified by the two separate methodologies.

Organization	Yes or No	Question 4 Comment
Response: Newly Registered Entity Scenarios, Scenario 3a: It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of riskbased methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.		
Consolidated Edison Company of New York INC.	Yes	In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph? A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached.? Should be deleted for the following reasons: It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. "at least annually"), an entity understand that the Responsible Entity is compliant with the requirement if it can produce demonstration of completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example) and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually.CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan.CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the

Organization	Yes or No	Question 4 Comment
		compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order. This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Hydro-Québec TransEnergie (HQT) Independent Electricity System Operator Northeast Power Coordinating Council	Yes	In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph: "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached. should be deleted for the following reasons: It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. "at least annually"), an entity understands that the Responsible Entity is compliant with the requirement if it can demonstrably produce completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example), and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually.CIP-008-2/3

Organization	Yes or No	Question 4 Comment
		R1.6: the required records demonstrating the annual exercise of the incident response plan.CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at the Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order."This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Orange and Rockland Utilities Inc	Yes	In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph states: A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to

Organization	Yes or No	Question 4 Comment
		demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached. This statement should be deleted for the following reasons: It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. “at least annually”), an entity understand that the Responsible Entity is compliant with the requirement if it can produce demonstration of completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example) and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually.CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan.CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date.? It is outside of the scope of the SAR. In its Order, the FERC’s directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order. This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly		

Organization	Yes or No	Question 4 Comment
Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
E.ON U.S. LLC	Yes	Modify requirement R1.6.1 to read as follows: R1.6.1 Visitor logs. Utilizing less prescriptive language in this requirement will provide Responsible Entities with the flexibility to reasonably apply the standard to each of the various circumstances that exist in the industry. For example, providing continuous escorts for parties that don't have unrestricted access to the critical cyber equipment or facilities requires additional staffing. Due to, for example, the number of potential contractors that may be "on-site" at any given time, numerous escorts may be required. The use of a "monitor" would not be sufficient because the escort must have enough knowledge to determine if a cyber incident is occurring. E.ON U.S. favors a process whereby contractors procure critical access certification from NERC or the RRO.
Response: The modification suggested by E.ON U.S. does not adequately meet the FERC directive "to develop a modification to Reliability Standard CIP-006-2 … to add a requirement of a visitor control program, including the use of visitor logs to document entry and exit…"		
Progress Energy	Yes	Progress Energy intends to vote Negative in the upcoming ballot primarily because it disagrees with the proposed language in CIP-006-3a, R1.6.1. Specifically, Progress does not agree with the requirement to document the visitor's time and date of exit from Physical Security Perimeters. Progress is aware of the FERC order issued September 30, 2009 which requires logging of entry and exit dates and times for escorted visitors. Nevertheless, as a practical matter, for facilities with multiple PSPs such as large power plants, it is not feasible to maintain visitor logs for egress when frequent daily or hourly entries to/exits from such PSPs occur, such as during an outage. More importantly, Progress believes that the value of an authorized escort is to maintain continuous surveillance, accountability, and control over the visitor whenever the visitor is within the PSP. Requiring the logging of egress dates and times for escorted visitors does not provide any additional CIP benefit because it does not improve the security of the PSP in real time. It would, however, greatly increase cost, reduce productivity, and create opportunity for inadvertent violation of the NERC requirement. FERC did not order that personnel with unescorted access also be required to log egress times and dates, presumably because there is no benefit to doing so. Likewise, if the escort is properly performing his/her function, there would be no reason to log egress times and dates for those being escorted.
Response: The SDT does not agree that the requirement to log the ingress and egress of visitors from Physical Security Perimeters greatly increases costs and reduces productivity. It is the opinion of the SDT that documenting precisely when unauthorized individuals had escorted access inside Physical Security Perimeters is a key element of an acceptable visitor control program. Outages due to emergencies may be addressed by CIP-003 R1 (Policy), and in CIP-004 R2 and R3 (Training and Personnel Risk Assessment). The SDT reminds the entity that it also has the discretion to grant an		

Organization	Yes or No	Question 4 Comment
individual authorized unescorted physical access to the Physical Security Perimeter should the requirement of escorting and logging ingress and egress prove burdensome.		
NextEra Energy Resources Silvia Parada-Mitchell Florida Power & Light	Yes	Regarding CIP-006-3a, R1.6.1 specifically, we do not agree with the requirement to document the visitor's time and date of exit from Physical Security Perimeters. Facilities with multiple PSPs such as large power plants, it is not feasible to maintain visitor logs for egress when frequent daily or hourly entries to/exits from such PSPs occur, such as during an outage. We believe the value of an authorized escort is to maintain continuous surveillance, accountability, and control over the visitor whenever the visitor is within the PSP. Requiring the logging of egress dates and times for escorted visitors does not provide any additional CIP benefit because it does not improve the security of the PSP in real time. It would, however, greatly increase cost, reduce productivity, and create opportunity for inadvertent violation of the NERC requirement.
Response: The SDT does not agree that the requirement to log the ingress and egress of visitors from Physical Security Perimeters greatly increases costs and reduces productivity. It is the opinion of the SDT that documenting precisely when unauthorized individuals had escorted access inside Physical Security Perimeters is a key element of an acceptable visitor control program. Outages due to emergencies maybe addressed by CIP-003 R1 (Policy), and in CIP-004 R2 and R3 (Training and Personnel Risk Assessment). The SDT reminds the entity that it also has the discretion to grant an individual authorized unescorted physical access to the Physical Security Perimeter should the requirement of escorting and logging ingress and egress prove burdensome.		
PacifiCorp	Yes	Regarding the implementation plan treatment of merging Responsibilities Entities: when combining separate risk-based methodologies, PacifiCorp believes that each separate methodology should be applied to the combined system and the methodology that provides the most robust level of protection against a cyber attack based on the critical assets identified should be selected. The selected methodology should be applied to the combined system with no requirement that the resultant list contain all of the critical assets previously identified by the two separate methodologies.
Response: It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of risk-based methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.		
Portland General Electric Company	Yes	The Draft Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities contains the following statement: "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." PGE strongly disagrees with this approach. PGE believes that this language

Organization	Yes or No	Question 4 Comment
		directly contradicts the plain language understanding of an "annual" requirement, and this is made clear by reference to the Standards currently under consideration. Looking at Standard CIP-003-3 R4 (Information Protection), for example, a Responsible Entity "shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets." It is clear, then, that a Registered Entity must have in place an Information Protection Program on or before the "Compliant" milestone date. However, R4.3 of this Standard provides that 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." (Emphasis added.) This R4.3 clearly contemplates an "assessment" of the information protection program that takes place after the initial implementation of that program and recurs "annually" thereafter. Applying the interpretation of "annual" set forth in the Draft Implementation Plan to this Standard, an entity would have to "implement and document" a program, and also "assess adherence" to that same program by the "Compliant" milestone date. Determining adherence to a new program requires that the program be in place and exercised for a period of time, otherwise you do not have enough relevant data to "assess adherence". Similarly, in Standard CIP-007-3 R8 (Cyber Vulnerability Assessment), a Responsible Entity "shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually." Looking at the sub requirements within this R8, it is clear that this "annual" review requirement is triggered after the "Compliant" milestone date. Requirement 8.2, for example, requires the entity to "verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled." This requirement pertaining to ports and services is set forth separately in R2 of the same Standard. As such, the plain language interpretation of this Standard is that an entity must establish compliance with the stand-alone R2 requirement pertaining to ports and services on or before the "Compliant" milestone date, and then perform a Cyber Vulnerability Assessment annually thereafter to test ongoing compliance. If the Cyber Vulnerability Assessment (R8) must be performed for the first time on or before the "Compliant" milestone date, then it is duplicative of other requirements within the Standard. It is clear, then, that a requirement to perform an action on an annual basis gives the entity a year from the time that the requirement reaches the Compliant milestone date for the first instance of performing that action. The Standard Drafting Team's approach would require a utility to comply with the requirement before the Compliant milestone date, rendering the Compliant milestone date meaningless. An entity has not failed to meet the requirement until it fails to complete the requirement activity on an annual basis. By definition this cannot take place until two conditions have been met: (1) the requirement has been mandatory on the entity (i.e., at the Compliant stage); and (2) the entity has failed to perform the requirement activity at least as often as once a year. The entity's failure to perform the activity prior to expiration of the "annual" period following the Compliant milestone cannot constitute noncompliance because the activity can still be taking place on an annual basis. Construing all requirements with a prescribed periodicity to require the first performance of the requirement activity prior to the Compliant milestone can undermine the intent of the standard, which is for the registered entity to perform the activity in keeping with their typical annual performance cycles. For example,

Organization	Yes or No	Question 4 Comment
		a requirement that reaches the "Compliant" milestone on January 1 can include an annual performance activity that the entity typically does as part of an outage drill which is done every September. The entity should not be forced to alter their typical annual schedule in order to meet the requirement before it has reached the "Compliant" stage. This approach is not supported by past standard development activity or by FERC Order and represents a fundamental shift in NERC's approach to such requirements with prescribed periodicities. Given that many such requirements are currently or will soon be at the Compliant milestone date, such a shift in approach would require adequate notice to the affected entities.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Manitoba Hydro	Yes	The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was significantly changed after approval by industry and the NERC BOT. The changes, pertaining to periodic requirements, were not directed by FERC in Order 706 or Order RD09-7-000, or through industry comments. The changes require that for a number of requirements, which were not specified by NERC, with " a prescribed periodicity" the first occurrence of the recurring requirement must be completed by the Compliant milestone date??, which could advance the need to meet the requirements up to a year. This is not the general understanding of the industry, and was not the guidance provided in the NERC (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1. From the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 document provided with the Version 1 standards, "Compliant means that the entity meets the full intent of the requirements, and is beginning to maintain required "data", "documents", "logs", and "records". Auditably Compliant means that the entity meets the full intent of the requirements and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data", "documents", "logs", and "records"." Meeting the intent of the requirements means that the processes, procedures and infrastructure are in place to begin collecting data during the Auditably Compliant period. A quarterly review should not need to be conducted before the Compliant date; it is completed, at latest, at the end of the first quarter of the compliance period. The direction provided in the new Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is unclear and inconsistent, as some unspecified requirements with a prescribed periodicity must have their first periodic occurrence completed by the compliance date, while other unspecified periodic requirements can begin collection of their respective data by the compliance date. It is too late to introduce new compliance direction for standards whose initial compliance dates will have passed by the time the

Organization	Yes or No	Question 4 Comment
		Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is approved. We recommend the removal of the paragraph on Page 2 which begins “A number of the NERC Reliability Standard requirements include a prescribed periodicity “. With the removal of that paragraph, the following paragraphs in that section are unnecessary and should also be removed.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Dominion Virginia Power	Yes	The proposed requirement CIP-006-3a R1.6.1 is redundant to and/or conflicts with requirement R6. A suggested modification: R1.6 Each PSP shall be governed by a visitor control program which, at a minimum, provides the following requirements: R1.6.1 Continuous escorting of any personnel without authorized unescorted access to the PSP R1.6.2 Meets the logging requirements found in CIP-006-3a R6. If the above change is not considered, please amend CIP-006-3a R6 to indicate that it only applies to non-visitors.
Response: The SDT clarifies that Requirement CIP-006 R1.6 specifies a visitor control program. Under this requirement, the “visitor’s identity, time and date of entry to and exit from Physical Security Perimeters” must be logged. The SDT did not modify the requirements for individuals with authorized unescorted access to the Physical Security Perimeter. CIP-006 R6 requires a log that captures “time of access” for all individuals who enter a Physical Security Perimeter. Project 2008-15 “Interpretation of CIP-006-1a By US Army Corps of Engineers” clarifies that the term “time of access” indeed refers to the time an authorized individual enters the physical security perimeter.		
Silicon Valley Power	Yes	Violation Severity Levels in some cases do not provide for either Moderate or Low levels in all cases
Response: Not all requirements have four violation severity levels. Note that the impact to reliability of a requirement is measured by the VRF; the VSL is an indication of the lack of compliance with the requirement.		
Midwest ISO Standards Collaborators	Yes	We agree that the modifications to the standards and implementation plans meet the intent of the FERC directives but do have some suggestions for improving them. 1) In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Organization	Yes or No	Question 4 Comment
		document, Category 1 Scenario under Newly Registered Entity Scenarios on page 8 appears to address what is largely a registration issue. It appears that the document assumes that the merging entities will join their registration but this may not be the case. There is no NERC rule that requires two utilities that operate separate balancing authorities to merge those balancing authorities once the merger is completed. They may continue to be registered as two BAs as a result. Consider the Duke-Cinergy merger as example of when this happened. The scenario should be updated to consider these issues or to identify the assumptions made. Further, we suggest the that the last two sentences in the second paragraph under the Category 1 Scenario beginning with following language should be deleted as a result: "it would be preferred that a single program be the result of this analysis, however,". 2) In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, the first sentence (as shown below) in the second paragraph in section (a) under the Category 3 Scenario under Newly Registered Entity Scenarios should be deleted. That sentence is: "Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets." This sentence assumes that the primary purpose of the CIP standards is to protect the Critical Cyber Assets and that once a Critical Cyber Asset always a Critical Cyber Asset. Rather, the purpose is to protect the grid by ensuring it can't be compromised by hacking of a cyber asset. It demonstrates ignorance that how the grid is operated can, will and should affect the Critical Asset list. Mergers can affect how the grid is operated and ultimately the Critical Asset list. As an example, a merged utility may combine its two previously separate Balancing Authorities into a single Balancing Authority. This would cause the Contingency Reserve obligation to increase and could cause a generating unit to be no longer a Critical Asset as a result. Table C-2 in NERC's Security Guideline for the Electricity Sector: Identifying Critical Assets document specifically identifies a unit exceeding the Contingency Reserve obligation as a reason to classify a generating unit as a Critical Asset. This is hardly an extraordinary circumstance. Further, this outcome would occur even if the two merged entities had identical Critical Asset identification methodologies. 3) In an August 10, 2009 informational filing to FERC, NERC laid out a new approach to define one VRF at the requirement level that applies to the requirement and its sub-requirements and applies a single comprehensive set of VSLs to the main requirement that categorizes non-compliance with the main requirement and sub-requirement. This approach should be applied here. 4) The VRFs on CIP-006-3a R1.6 and R1.6.1 should be Lower because it is completely an administrative requirement intended to demonstrate to the Commission that visitors are escorted. Failure to have a visitor control program that includes logs is hardly a risk especially when one considers that other requirements such as CIP-006-3a R4 already mandate that a secure perimeter would be maintained. With R4 in place, a visitor

Organization	Yes or No	Question 4 Comment
		could not gain unnecessary access even if there were no visitor log maintained. 5) For the VSLs on CIP-006-3a R1.6, a potential non-compliance that is likely to occur that is not considered is for the case of not logging egress when ingress is logged. VSLs could be written based on the number of visitors that don't have egress logged. Likely, if ingress is not logged, egress will not be logged and no record of the visitor will exist. For this reason, the Moderate and High VSLs will likely never apply. The Moderate VSL appears to assume that the compliance auditor will be able to review a record of all visitors that were not logged into the visitor log. The visitor log is intended to be the record of visitors so how will the compliance auditor know a visitor wasn't logged. No evidence would exist. 6) We suggest the following wording for CIP-006-3a R1.6.1 would be more succinct and provide the same meaning. "Visitor logs to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of the escort with authorized unescorted physical access performing the escort." 7) The drafting team should consider defining the term visitors in R1.6 and eliminating the clause in parentheses. Clauses like these could be misconstrued from its intention which is to define visitor. A definition is cleaner and clearer.

Response:

1) **This section makes no assumption that merged companies or organizations automatically result in merged Registered Entities. It describes a situation when two Responsible Entities merge into a single Responsible Entity: "A Merger of Two or More Registered Entities…." (emphasis inserted in this response).**

   Regarding the issue of preference for single program, the Implementation Plan expresses a preference and not a requirement. It is the opinion of the SDT that a single program reduces complexity for both the Responsible Entity and the compliance monitoring and enforcing organizations. Further, it reinforces that "Registered Entity specific circumstances may dictate or allow the two programs to continue separately."

2) **It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of risk-based methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.**

3) **The VSLs developed for the Version 3 standards are consistent with other VSLs for the existing Version 2 CIP Standards. The SDT will consider using the new VSL methodology in the next version of the standards.**

4) **It is the opinion of the SDT that facilities security is critically important, as also indicated by the Commission, and that visitor control programs and visitor logs are an essential element of sound facilities security. Therefore, it is the opinion of the SDT that a VRF of "Medium" is appropriate for**

Organization	Yes or No	Question 4 Comment
		R1.6 and R1.6.1. **5) The case of not logging egress when ingress is logged is considered under the Lower VSL as written. The SDT agrees that the cases of Moderate and High VSLs may be difficult to identify as a finding during an audit, but are in fact likely scenarios that may be self-reported by the entity. In addition, while the visitor log is the record of visitors, there may be other records available such as video recordings of a PSP that may show that a visitor entered without completing the required log information.** **6) The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.** **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.** **7) The SDT agrees that definitions in the NERC glossary provide clean and clear information to the entity. However, definitions in the glossary must also apply across all NERC standards and thus often have unintended consequences. In the case of the definition of visitors, it is the opinion of the SDT that the parenthetical definition is clear enough to not be misconstrued from its intention.**
Duke Energy	Yes	We support the MISO Standards Collaborators' comments, and have the following additional comments: 1. NERC: V3 Implementation Plan: The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard. Can the industry have some kind of an estimate as to when that will be 2. Implementation Plan for Newly Identified Critical Assets. Comment/question to NERC. Utilities really want to do the right thing. It is quite possible that new Critical Assets may be identified late in 2009. CIP version 1 has no implementation plan for such new identified Critical Assets, and NERC acknowledges this “compliance gap”. An implementation plan to address this gap is being proposed here. This same implementation plan was proposed in v2. A compliance gap exists for newly identified CA until this proposed effective date. This implementation plan for newly identified Critical assets is desperately needed by the utility. The implementation plan was poorly written when submitted by NERC to FERC and was, therefore, not included in the FERC approved Version 2 materials. This is no fault of the utilities. What is the proposed effective date of the Implementation Plan for Newly Identified Critical Assets? If a utility has newly identified Critical Assets between the compliance date for CIP version 1 and the effective date of the Implementation Plan for Newly Identified Assets, what schedule should they follow for the implementation of CIP? It is not reasonable to expect that newly identified Critical Assets are immediately “auditably compliant” under CIP version 1. What remedy is available to the utilities short of non-compliance related to newly identified Critical Assets prior to the effective date of this Implementation Plan? 3. Version 1 Implementation Plan Retirement: The Version 1 Implementation Plan will be retired once all

Organization	Yes or No	Question 4 Comment
		Entities in Tables 1, 2, and 3 of that plan have achieved their Compliant state. "The wording in the NERC material states that Version 1 Implementation Plan will not be retired until the Entities achieve compliant state. Is this true" Shouldn't the posting read "Version 1 Implementation Plan will be retired once the target dates explained in the Phased In Plan expire"? 4. Dropping "Auditably Compliant". The term "auditably compliant" has been dropped from this future version of the implementation plan. We do not object, but we have a clarifying question: Auditably compliant referred to the need to have 12 months of data. At what point is the utility expected to have 12 months of data accumulated for review during an audit? Is it at the compliant stage or 12 months subsequent to compliant stage?

Response:

1) **NERC has no control over when various milestones in the regulatory approval process can be achieved. The effective date formula is based on the date of regulatory approval.**
2) **FERC approved the Implementation Plan for Newly Identified Critical Cyber Assets in its order approving the Version 2 CIP Standards. These are effective April 1st, 2010. The SDT acknowledges there is a compliance gap, and in the period after an entity's compliance date and extending to April 1, 2010, this issue should be addressed through the Compliance Monitoring and Enforcement Program.**
3) **The wording in the "Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3" has been clarified.**
4) **This issue is a compliance issue which must be addressed by NERC Compliance. The paragraph in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities has been removed.**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool and Pre-ballot Window
October 27–November 20, 2009

Now available at: https://standards.nerc.net/BallotPool.aspx

Project 2009-21: Cyber Security Ninety-day Response

Proposed critical infrastructure protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3 are posted for a pre-ballot review. A general implementation plan for these standards and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* are also posted. Registered Ballot Body members may join the ballot pool to be eligible to vote on this interpretation **until 8 a.m. EDT on November 20, 2009**.

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list server for this ballot pool is: bp-2009-21_CS-90_in.

Special Notes for this Pre-ballot Window

Due to the Federal Energy Regulatory Commission (FERC) directive to develop and file modifications to the CIP Reliability Standards within 90 days of its September 30, 2009 order, the Standards Committee authorized deviations from the standards development process. This pre-ballot review will overlap the comment period that is already underway and will be followed by the initial ballot for the standards and implementation plans. Prior to the initial ballot, the drafting team will draft and post responses to comments received.

Project Background

The purpose of this project is to modify certain CIP Reliability Standards in response to the directives issued in the FERC September 30, 2009 order approving version 2 of the CIP standards. The revised standards include associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

Standards Development Process

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

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Initial Ballot Window Open
November 20–30, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Project 2009-21: Cyber Security Ninety-day Response

An initial ballot window for proposed critical infrastructure protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3, a general implementation plan, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* is now open **until 8 p.m. EST on November 30, 2009**.

Special Notes for this Ballot Window

Due to the Federal Energy Regulatory Commission (FERC) directive to develop and file modifications to the CIP Reliability Standards within 90 days of its September 30, 2009 Order, the Standards Committee authorized deviations from the standards development process, which included an allowance for a concurrent ballot-pool formation and comment period. The drafting team has posted responses to comments received and has made revisions to proposed standard CIP-006-3 and both implementation plans to address stakeholder concerns. The revisions are summarized below:

1. CIP-006-3: the drafting team revised CIP-006-3 Requirement R1.6 to more fully address the directive included in the FERC Order approving Version 2 CIP Standards issued September 30, 2009.
2. *Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3*: in order to provide additional clarity, the drafting team modified the section of the plan that addresses retirement of earlier implementation plans.
3. *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities*: several stakeholders asked for clarity regarding language concerning the date of first occurrence of a recurring requirement. The drafting team acknowledged that the initial date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective, and the team has removed the language from the implementation plan. NERC compliance staff is expected to issue a compliance bulletin addressing this issue.

A detailed description of the changes is included in the consideration of comments document posted on the project page:
http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

We understand this ballot will span the U.S. Thanksgiving holiday. However, in order to meet the FERC-imposed 90-day deadline, NERC believes this is a necessary inconvenience. Other current open ballot windows of less urgency will be extended to allow entities to focus on this ballot.

Instructions
Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Next Steps
Voting results will be posted and announced after the ballot window closes.

Project Background
The purpose of this project is to modify certain CIP Reliability Standards in response to the directives issued in the FERC September 30, 2009 Order approving version 2 of the CIP standards. The revised standards include associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).

Applicability of Standards in Project
Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

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

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3

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

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

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

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "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-002-3:

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.

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

1.5.1 None.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	

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.

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).

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

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

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

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

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, 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.

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-3

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

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

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

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

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

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

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program**.** Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	

A. Introduction

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

2. Number: CIP-005-3

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 a 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.

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		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity.	

		Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

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.

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-003-3 Requirement R5 and Standard CIP-004-3 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-008-3.

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-005-3.

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

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

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

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

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

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

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

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

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 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. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	

A. Introduction

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

2. Number: CIP-008-3

3. Purpose: Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-23should 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-008-3, "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-008-3:

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

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

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

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

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

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

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

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

C. Measures

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-3 for the previous full calendar year unless directed by its Compliance Enforcement

Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

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

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

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

2. Number: CIP-009-3

3. Purpose: Standard CIP-009-3 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-3 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-009-3, "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-009-3:

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~2~~3

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

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

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

Standard CIP-002-~~2~~3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-~~2~~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-002-~~2~~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.

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-~~2~~3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-~~2~~3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

1.5.1 None.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Updated version number from -2 to -3	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Font: Verdana, 10 pt
Formatted: Font: Verdana, 10 pt
Formatted: Font: Verdana, 10 pt
Formatted: Left
Formatted: Font: Verdana, 10 pt

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~2~~3

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

4. **Applicability:**

   4.1. Within the text of Standard CIP-003-~~2~~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-~~2~~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-~~2~~3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-~~2~~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-~~2~~3 through CIP-009-~~2~~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.

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

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-~~2~~3 through CIP-009-~~2~~.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-~~2~~3 through CIP-009-~~2~~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).

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

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

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

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

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-~~2~~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.

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Update version number from -2 to -	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Font: 10 pt
Formatted: Left

		3	

A. Introduction

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

2. **Number:** CIP-004-~~2~~3

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

4. **Applicability:**

   4.1. Within the text of Standard CIP-004-~~2~~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-004-~~2~~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-~~2~~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. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

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

Formatted: French (France)

Formatted: French (France)

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

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

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

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-~~2~~3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-~~2~~3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program**.** Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Update version number from -2 to -3	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Left
Formatted: Table Col Heading
Formatted: Font: Times New Roman, Not Bold
Formatted: Font: Times New Roman
Formatted: Table Col Heading, Left
Formatted: Font: 10 pt

Formatted: Bottom: 0.5"

A. Introduction

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

2. Number: CIP-005-~~2~~3

3. Purpose: Standard CIP-005-~~2~~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-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. Applicability

4.1. Within the text of Standard CIP-005-~~2~~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-~~2~~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-~~2~~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-~~2~~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 a specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3 Requirement R3; Standard CIP-007-~~2~~3 Requirements R1 and R3 through R9; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~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-~~2~~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.

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

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

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

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

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

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

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

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

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

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-~~2~~3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-~~2~~3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-~~2~~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-~~2~~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-~~2~~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-~~2~~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		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.	

Formatted: Left
Formatted Table
Formatted: Left
Formatted: Left

		Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Update version from -2 to -3	~~Revised~~

Formatted: Font: Times New Roman, Not Bold

Formatted: Table Col Heading

Formatted: Font: Times New Roman, Not Bold

Formatted: Table Col Heading, Left

Formatted: Font: 10 pt, Not Bold

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1.Conduct initial ballot	April 2 - 11, 2009
2.Post response to comments on first ballot	April 20 - May 12, 2009
3.Conduct recirculation ballot	May 13 - 22, 2009
4.Board adoption date.	To be determined.

A. Introduction

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

2. **Number:** CIP-006-~~2~~3

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

4. **Applicability:**

4.1. Within the text of Standard CIP-006-~~2~~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-006-~~2~~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-~~2~~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. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

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

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

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

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

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter ~~of personnel not authorized for unescorted access.~~.

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

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

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

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3 Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.

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

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

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures

specified in Requirement CIP-008-~~2.~~3. One or more of the following monitoring methods shall be used:

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

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

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

R7. Access Log Retention — The ~~responsible entity~~Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-~~2~~3 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	

Formatted: Bottom: 0.5"

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~2~~3

3. Purpose: Standard CIP-007-~~2~~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-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. Applicability:

4.1. Within the text of Standard CIP-007-~~2~~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-~~2~~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-~~2~~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-~~2~~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-~~2~~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-~~2~~3 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-~~2~~3 Requirement R5 and Standard CIP-004-~~2~~3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-~~2~~3.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-~~2~~3.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-~~2~~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-~~2~~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	

Formatted: Left

Formatted Table

		Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Updated version numbers from -2 to -3	~~Revised~~

Formatted: Font: 10 pt

Formatted: Left

Formatted: Font: 10 pt

Formatted: Left

Formatted: Font: 10 pt

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-~~2~~3

3. **Purpose:** Standard CIP-008-~~2~~3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-~~2 should~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. **Applicability**

   4.1. Within the text of Standard CIP-008-~~2~~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-008-~~2~~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-~~2~~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. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. ~~Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.~~

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-~~2~~3 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~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.	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Font: 10 pt
Formatted: Left
Formatted: Left
Formatted: Font: 10 pt

Formatted: Bottom: 0.5"

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for Critical Cyber Assets

2. **Number:** CIP-009-~~2~~3

3. **Purpose:** Standard CIP-009-~~2~~3 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. **Applicability:**

   4.1. Within the text of Standard CIP-009-~~2~~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-009-~~2~~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-~~2~~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. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-~~2~~3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
~~2~~3	~~05/06/09~~	~~Adopted by NERC Board of Trustees~~Updated version numbers from -2 to -3	~~Revised~~

Formatted: Left
Formatted Table
Formatted: Font: 10 pt
Formatted: Left
Formatted: Left
Formatted: Font: 10 pt

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-3

3. Purpose: Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 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-006-3, "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-006-3:

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. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures

specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1.Conduct initial ballot	April 2 - 11, 2009
2.Post response to comments on first ballot	April 20 - May 12, 2009
3.Conduct recirculation ballot	May 13 - 22, 2009
4.Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets

2. **Number:** CIP-006-~~2~~3

3. **Purpose:** Standard CIP-006-~~2~~3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. **Applicability:**

4.1. Within the text of Standard CIP-006-~~2~~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-006-~~2~~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-~~2~~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. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter ~~of personnel not authorized for unescorted access.~~.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3 Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures

specified in Requirement CIP-008-~~2.~~3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The ~~responsible entity~~Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-~~2~~3 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.
8. Posted for Stakeholder Comment from November 20, 2008 to January 5, 2009.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

- CIP-002-1 — Cyber Security — Critical Cyber Asset Identification
- CIP-003-1 — Cyber Security — Security Management Controls
- CIP-004-1 — Cyber Security — Personnel and Training
- CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)
- CIP-006-1 — Cyber Security — Physical Security
- CIP-007-1 — Cyber Security — Systems Security Management
- CIP-008-1 — Cyber Security — Incident Reporting and Response Planning
- CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards is for pre-ballot review. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1.Conduct initial ballot	April 2 - 11, 2009
2.Post response to comments on first ballot	April 20 - May 12, 2009
3.Conduct recirculation ballot	May 13 - 22, 2009
4.Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets

2. **Number:** CIP-006-~~2~~3

3. **Purpose:** Standard CIP-006-~~2~~3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-~~2~~3 should be read as part of a group of standards numbered Standards CIP-002-~~2~~3 through CIP-009-~~2~~3.

4. **Applicability:**

4.1. Within the text of Standard CIP-006-~~2~~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-006-~~2~~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-~~2~~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. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter ~~of personnel not authorized for unescorted access.~~.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~3 Requirement R3; Standard CIP-005-~~2~~3 Requirements R2 and R3; Standard CIP-006-~~2~~3 Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures

specified in Requirement CIP-008-~~2.~~3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The ~~responsible entity~~Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-~~2~~3 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points.Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–3 — Cyber Security — Critical Cyber Asset Identification
CIP–003–3 — Cyber Security — Security Management Controls
CIP–004–3 — Cyber Security — Personnel and Training
CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–3 — Cyber Security — Physical Security
CIP–007–3 — Cyber Security — Systems Security Management
CIP–008–3 — Cyber Security — Incident Reporting and Response Planning
CIP–009–3 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Proposed Effective Date

The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 3 of the NERC Cyber Security Standards CIP-002-3 to CIP-009-3.

Prior Version Implementation Plan Retirement

By December 31, 2009, CIP Version 1's Table 1, 2, and 3 Registered Entities that registered prior to December 31, 2007 will have reached the "Compliant" milestone for all CIP Version 1 Requirements. Timetables for reaching the "Auditably Compliant" milestone will still be in effect for these Entities going forward until said timetables expire. As such, when Table 3 Registered Entities reach the Auditably Compliant milestone on December 31, 2010, the Version 1 Implementation Plan is in practice retired. Table 4 of the CIP Version 1 Implementation Plan is applicable only for newly Registered Entities, and compliance milestones for newly Registered Entities is included in CIP Version 2's Implementation Plan for Newly Identified Critical Cyber

Assets and Newly Registered Entities effective on April 1, 2010. CIP Version 3 milestones, are effective after FERC approval.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version ~~2~~3 of Cyber Security Standards CIP-002-~~2~~3 through CIP-009-~~2~~3

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

~~Modified~~Applicable Standards

The following standards ~~have been modified~~are covered by this Implementation Plan:

CIP–002–~~2~~3 — Cyber Security — Critical Cyber Asset Identification
CIP–003–~~2~~3 — Cyber Security — Security Management Controls
CIP–004–~~2~~3 — Cyber Security — Personnel and Training
CIP–005–~~2~~3 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–~~2~~3 — Cyber Security — Physical Security
CIP–007–~~2~~3 — Cyber Security — Systems Security Management
CIP–008–~~2~~3 — Cyber Security — Incident Reporting and Response Planning
CIP–009–~~2~~3 — Cyber Security — Recovery Plans for Critical Cyber Assets

~~Red-line versions of the above~~These standards are posted for ballot by NERC together with this Implementation Plan. When these ~~modified~~ standards become effective, ~~the~~all prior versions of these standards ~~and their Implementation Plan~~ are retired.

Compliance with Standards

Once these standards become effective, the ~~responsible entities~~Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

- NERC
- Regional Entity

~~Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.~~

Proposed Effective Date

~~The proposed effective date for these modified standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters) after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).~~

~~For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.~~

The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 3 of the NERC Cyber Security Standards CIP-002-3 to CIP-009-3.

Prior Version Implementation Plan Retirement

By December 31, 2009, CIP Version 1's Table 1, 2, and 3 Registered Entities that registered prior to December 31, 2007 will have reached the "Compliant" milestone for all CIP Version 1 Requirements. Timetables for reaching the "Auditably Compliant" milestone will still be in effect for these Entities going forward until said timetables expire. As such, when Table 3 Registered Entities reach the Auditably Compliant milestone on December 31, 2010, the Version 1 Implementation Plan is in practice retired. Table 4 of the CIP Version 1 Implementation Plan is applicable only for newly Registered Entities, and compliance milestones for newly Registered Entities is included in CIP Version 2's Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities effective on April 1, 2010. CIP Version 3 milestones, are effective after FERC approval.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–3 — Cyber Security — Critical Cyber Asset Identification
CIP–003–3 — Cyber Security — Security Management Controls
CIP–004–3 — Cyber Security — Personnel and Training
CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–3 — Cyber Security — Physical Security
CIP–007–3 — Cyber Security — Systems Security Management
CIP–008–3 — Cyber Security — Incident Reporting and Response Planning
CIP–009–3 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Proposed Effective Date

The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 3 of the NERC Cyber Security Standards CIP-002-3 to CIP-009-3.

Prior Version ~~1~~ Implementation Plan Retirement

~~The Version 1 Implementation Plan will be retired once all Entities in Tables 1, 2, and 3 of that plan have achieved their Compliant state.~~

~~Version 2 Implementation Plan Retirement~~

~~The Version 2 Implementation Plan will be retired on April 1, 2010 or on a Version 1 legacy date for compliance that goes beyond April 1, 2010, whichever is later.~~

By December 31, 2009, CIP Version 1's Table 1, 2, and 3 Registered Entities that registered prior to December 31, 2007 will have reached the "Compliant" milestone for all CIP Version 1 Requirements. Timetables for reaching the "Auditably Compliant" milestone will still be in effect for these Entities going forward until said timetables expire. As such, when Table 3 Registered Entities reach the Auditably Compliant milestone on December 31, 2010, the Version 1 Implementation Plan is in practice retired. Table 4 of the CIP Version 1 Implementation Plan is applicable only for newly Registered Entities, and compliance milestones for newly Registered Entities is included in CIP Version 2's Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities effective on April 1, 2010. CIP Version 3 milestones, are effective after FERC approval.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records."

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of either Version 2 or Version 3 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the risk-based Critical Asset identification methodology. Upon a subsequent annual application of the risk-based Critical Asset identification method in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, and Version 3) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2', or '-3') will be applied to that particular reference.
[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

In all cases where a *Compliant* milestone is specified in Table 2 (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant'[4]) one year following the *Compliant* milestone listed in this Implementation Plan.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC in April 2008 or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

---

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

[4] The term 'Auditably Compliant' (AC) used in this Implementation Plan for newly identified Critical Cyber Assets and newly Registered Entities means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" [see (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1]. Since in all cases, the 'Auditably Compliant' dates are one calendar year following the 'Compliant' (C) date, the Auditably Compliant dates are not specified in this plan. The terms 'Begin Work' (BW) and 'Substantially Compliant' (SC) used in the Version 1 Implementation Plan are no longer used, and therefore are not referenced in this Implementation Plan.

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by the Responsibility Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsibility Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commisioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on established criteria or thresholds in the Responsible Entity's existing risk-based Critical Asset identification method (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible

Entity.) Application of that risk-based Critical Asset Identification process is required annually (by CIP-002 R2), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

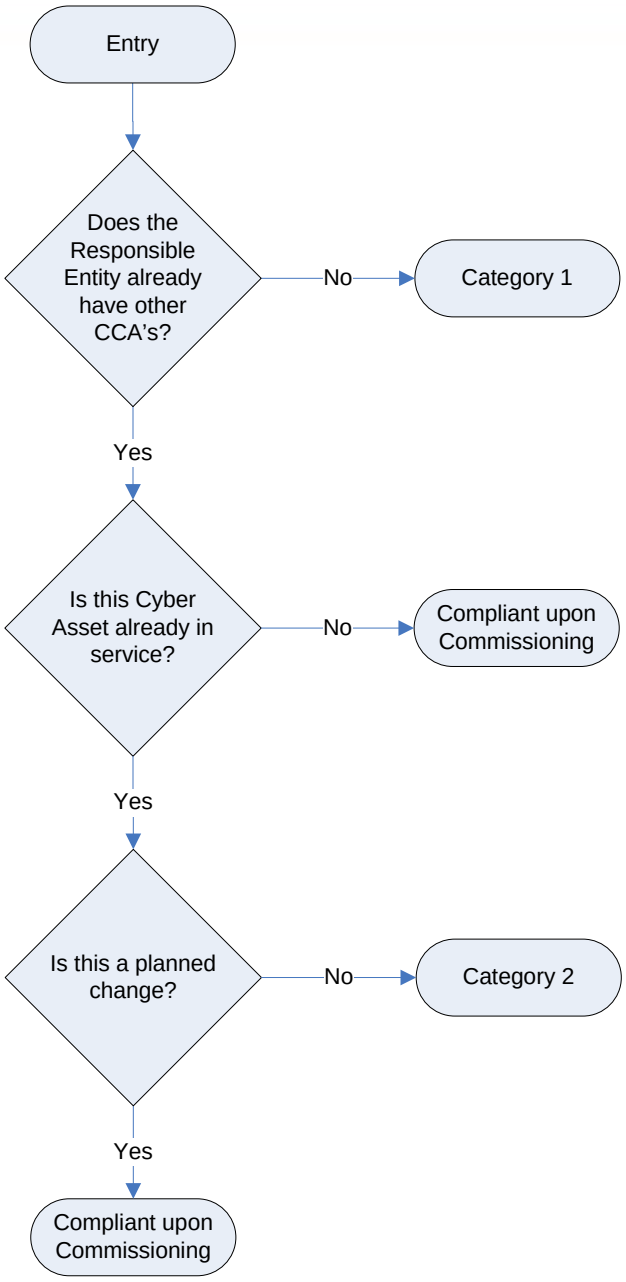


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on planning or impact studies) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to

demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is the NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology implementation by each predecessor Responsible Entity.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate risk-based Critical Asset identification methodology implementation while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of risk-based Critical Asset identification methodology(ies) as required in CIP-002 R2, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate methodologies, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the risk-based Critical Asset identification methodology as required in CIP-002 R2, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R3. If

newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

   Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

   A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing risk-based Critical Asset identification methodology and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as risk-based Critical Asset identification methodology. This scenario will be discussed in two sections, the first dealing with the combination of risk-based Critical Asset identification methodologies; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the risk-based Critical Asset identification methodologies: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate risk-based Critical Asset identification methodologies while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate the separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this

analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined risk-based Critical Asset identification methodology and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R2 and R3. If additional Critical Assets are identified as a result of the application of the merged risk-based Critical Asset identification methodology, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merge plan' must be made

available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated Critical Asset, but no newly designated Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5] Compliance Schedule for Standards CIP-002-2 through CIP-009-2 or CIP-002-3 through CIP-009-3 For Entities Registering in April 2008 and Thereafter				
	Registration + 12 months	Registration + 24 months		
	All Facilities	All Facilities		
CIP-002-2 or CIP-002-3 — Critical Cyber Assets				
All Requirements		Compliant		
Standard CIP-003-2 or CIP-003-3 — Security Management Controls				
All Requirements Except R2		Compliant		
R2	Compliant			
Standard CIP-004-2 or CIP-004-3 — Personnel & Training				
All Requirements		Compliant		
Standard CIP-005-2 or CIP-005-3 — Electronic Security				
All Requirements		Compliant		
Standard CIP-006-2 or CIP-006-3 — Physical Security				
All Requirements		Compliant		
Standard CIP-007-2 or CIP-007-3 — Systems Security Management				
All Requirements		Compliant		
Standard CIP-008-2 or CIP-008-3 — Incident Reporting and Response Planning				
All Requirements		Compliant		
Standard CIP-009-2 or CIP-009-3 — Recovery Plans				
All Requirements		Compliant		

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

~~**Implementation Plan for Cyber Security Standards CIP-003-1 through CIP-009-1 or Their Successor Standards**~~

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan ~~identifies~~applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records."

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for ~~becoming compliant~~compliance with the requirements of either Version 2 or Version 3 of the NERC Reliability Standards CIP-003~~-1~~ through CIP-009~~-1~~[1] on Cyber Security for (a) newly Registered Entities and ~~their successor standards, for assets determined to be~~(b) newly identified Critical Cyber Assets ~~once~~by an existing Registered Entity after the Registered Entity's applicable ~~'Compliant'~~ *Compliant* milestone date ~~listed in the existing Implementation Plan has~~has already passed.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan ~~specifies only a 'Compliant'~~defines the *Compliant* milestone~~. The Compliant milestone is expressed in this Implementation Plan table (Table 2) as the~~ dates in terms of the number of calendar months ~~following the~~after designation of the newly identified ~~asset~~ Cyber Asset as a Critical Cyber Asset, following the ~~requirements of~~ process stated in NERC Standard CIP-002~~-1 or its successor standard~~. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the risk-based Critical Asset identification methodology. Upon a subsequent annual application of the risk-based Critical Asset identification method in compliance with requirements of NERC

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, and Version 3) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2', or '-3') will be applied to that particular reference.
[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For ~~some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are~~ those NERC Reliability Standard requirements that have an entry in Table 2 annotated as ~~'0' herein. For other requirements~~*existing*, the designation of a newly identified Critical Cyber Asset has no bearing on ~~the~~its *Compliant* milestone date~~. These are annotated as *existing*~~, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

In all cases where a *Compliant* milestone ~~for compliance~~ is specified in Table 2 (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant'~~)~~[4]) one year following the *Compliant* milestone listed in this Implementation Plan~~. Where the milestone assumes prior compliance (i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones~~.

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

[4] The term 'Auditably Compliant' (AC) used in this Implementation Plan for newly identified Critical Cyber Assets and newly Registered Entities means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" [see (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1]. Since in all cases, the 'Auditably Compliant' dates are one calendar year following the 'Compliant' (C) date, the Auditably Compliant dates are not specified in this plan. The terms 'Begin Work' (BW) and 'Substantially Compliant' (SC) used in the Version 1 Implementation Plan are no longer used, and therefore are not referenced in this Implementation Plan.

~~**There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.**~~

~~Implementation Schedule~~

~~**There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:**~~

~~**A Cyber Asset becomes the first**~~ Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC in April 2008 or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset ~~at a responsible Entity.~~ was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP ~~standards~~-003 through CIP-009, *not due to a planned change~~.~~ in the electric system or Cyber Assets by the Responsibility Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP ~~standards~~-003 through CIP-009, *due to a planned change in the electric system or Cyber*

Assets by the Responsibility Entity. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the ~~term~~phrase 'Cyber Asset becomes subject to the ~~CIP standards'~~NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commisioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on established criteria or thresholds in the Responsible Entity's existing risk-based Critical Asset identification method (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of that risk-based Critical Asset Identification process is required annually (by CIP-002 R2), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

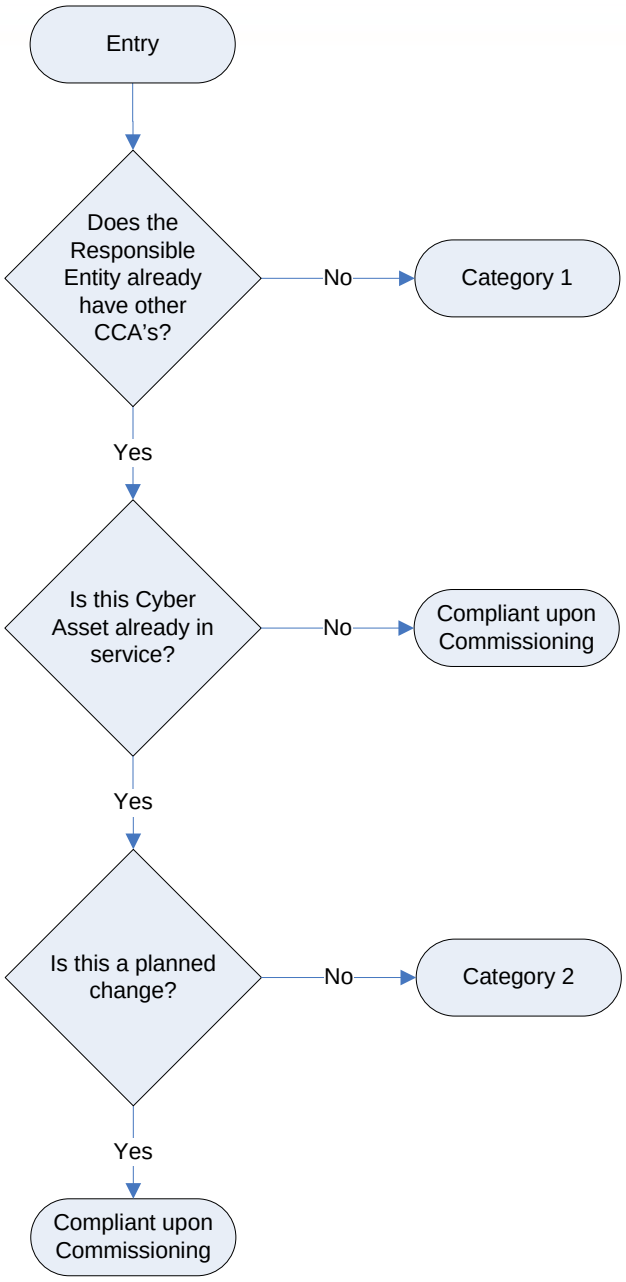


Figure 1: Category Selection Process Flow

~~**The individual categories are distinguished as follows:**~~

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with ~~-~~Critical Assets, but has now identified one or more Critical Cyber Assets. ~~The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-003-1 through CIP-009-1.)~~ As such, it is presumed that the Responsible Entity ~~has no~~ does not have a previously established ~~cyber security~~CIP compliance implementation program ~~in force. Table 3 also shall apply~~.

~~1.~~ The *Compliant* milestones defined for this Category are defined in ~~the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.~~

Table 2 (Milestone Category ~~2~~1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established ~~CIP Compliance~~ NERC Reliability Standards CIP compliance implementation program ~~as required by an existing Implementation Schedule~~in place, and ~~now~~ has ~~added~~ newly identified additional ~~items~~existing Cyber Assets that need to be added to its Critical Cyber Asset list~~. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented~~ and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*~~, not when they are added or modified through construction, upgrade or replacement.~~ as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible

Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

~~In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.~~

~~In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.~~

Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established ~~CIP Compliance~~ NERC Reliability Standards CIP compliance implementation program ~~as required by an existing Implementation Schedule~~ and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

   a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on planning or impact studies) upon its commissioning or activation ~~(e.g., based on planning or impact studies).~~
   b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security ~~perimeter~~Perimeter) associated with a previously identified Critical Asset~~.~~
   ~~c) Addition of:~~
      ~~i. a Critical Cyber Asset, or,~~
   c) ~~an other~~Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
   d) Planned addition of:
      i. a Critical Cyber Asset, or,

ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter~~.~~

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP ~~Compliance Program as required by an existing Implementation Schedule~~compliance implementation program.

~~This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.~~

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the ~~responsible~~Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

~~Since the assets must be compliant upon commissioning, no milestones are provided herein.~~

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is the NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology implementation by each predecessor Responsible Entity.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate risk-based Critical Asset identification methodology implementation while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of risk-based Critical Asset identification methodology(ies) as required in CIP-002 R2, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate methodologies, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the risk-based Critical Asset identification methodology as required in CIP-002 R2, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R3. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing risk-based Critical Asset identification methodology and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as risk-based Critical Asset identification methodology. This scenario will be discussed in two sections, the first dealing with the combination of risk-based Critical Asset identification methodologies; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the risk-based Critical Asset identification methodologies: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate risk-based Critical Asset identification methodologies while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate the separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-

based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined risk-based Critical Asset identification methodology and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R2 and R3. If additional Critical Assets are identified as a result of the application of the merged risk-based Critical Asset identification methodology, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merge plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated ~~a~~ Critical Asset, but no newly designated Critical Cyber Assets. This

~~is~~situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with ~~these standards~~the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample ~~situations~~scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No ~~CIP~~ Program (note 1)	Existing ~~CIP~~ Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset ~~–~~ never before in service and not a replacement for an existing Cyber Asset ~~–~~ added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as ~~a~~ an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	~~1~~*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	~~*existing*~~6 months
R5	24 months	~~*existing*~~6 months
R6	24 months	~~*existing*~~6 months
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	~~6~~18 months
R3	24 months	~~6~~18 months
R4	24 months	~~6~~18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	~~0~~6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	~~0~~12 months
R3	24 months	~~0~~12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5] Compliance Schedule for Standards CIP-002-~~1~~2 through CIP-009-~~1~~2 or ~~Their Successor Standards~~CIP-002-3 through CIP-009-3 For Entities Registering in April 2008 and Thereafter				
~~Upon Registration~~	Registration + 12 months	Registration + 24 months	~~Registration + 36 months~~	
~~Requirement~~	All Facilities	All Facilities	~~All Facilities~~	~~All Facilities~~
CIP-002-~~1~~2 or CIP-002-3 — Critical Cyber Assets ~~or its Successor Standard~~				
All Requirements	~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-003-~~1~~2 or CIP-003-3 — Security Management Controls ~~or its Successor Standard~~				
All Requirements Except R2	~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
R2	~~SC~~Compliant	~~C~~	~~AC~~	~~AC~~
Standard CIP-004-~~1~~2 or CIP-004-3 — Personnel & Training ~~or its Successor Standard~~				
All Requirements	~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-005-~~1~~2 or CIP-005-3 — Electronic Security ~~or its Successor Standard~~				
All Requirements	~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-006-~~1~~2 or CIP-006-3 — Physical Security ~~or its Successor Standard~~				
All Requirements	~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-007-~~1~~2 or CIP-007-3 — Systems Security Management ~~or its Successor Standard~~				
All Requirements	~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~
Standard CIP-008-~~1~~2 or CIP-008-3 — Incident Reporting and Response Planning ~~or its Successor Standard~~				
All Requirements	~~BW~~	~~SC~~Compliant	~~C~~	~~AC~~

~~[5] The phase in of compliance in this table is identical to the phase in for CIP-002-1 through CIP-009-1 identified in Table 4 of the 2006 CIP Implementation Plan.~~[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

Standard CIP-009-~~1~~2 or CIP-009-3 — Recovery Plans ~~or its Successor Standard~~				
All Requirements	~~**BW**~~	~~**SC**~~**Compliant**	~~**C**~~	~~**AC**~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records."

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of either Version 2 or Version 3 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone ~~date~~dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the risk-based Critical Asset identification methodology. Upon a subsequent annual application of the risk-based Critical Asset identification method in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, and Version 3) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2', or '-3') will be applied to that particular reference.
[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009, in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

~~A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the~~ all cases where a *Compliant* milestone ~~date~~ is specified in Table 2~~. The entity is then~~ (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to ~~collect and maintain required "data," "documents," "documentation," "logs," and "records" to~~ demonstrate compliance ~~with the recurring requirement after~~(i.e., to be 'Auditably Compliant'[4]) one year following the *Compliant* milestone ~~date has been reached.~~

~~For those NERC Reliability Standard requirements that include a prescribed records retention period (e.g., retention of logs for 90 days), a Responsible Entity is expected to begin collection and retention of the required "data," "documents," "documentation," "logs," and "records" by the *Compliant* milestone date~~listed in ~~Table 2.~~

~~For retention requirements that are triggered by a specific event (e.g., a reportable incident), collection and retention of the required "data," "documents," "documentation," "logs," and "records" begins with the triggering event. In~~ this ~~instance, the requirement for records collection and retention does not begin until the *Compliant* milestone date in Table 2 is reached and only applies to triggering events occurring after the *Compliant* milestone date.~~

~~For those NERC Reliability Standard requirements that do not include a specified periodicity or records retention requirement, a Responsible Entity is expected to have available all records~~

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

[4] The term 'Auditably Compliant' (AC) used in this Implementation Plan for newly identified Critical Cyber Assets and newly Registered Entities means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" [see (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1]. Since in all cases, the 'Auditably Compliant' dates are one calendar year following the 'Compliant' (C) date, the Auditably Compliant dates are not specified in this plan. The terms 'Begin Work' (BW) and 'Substantially Compliant' (SC) used in the Version 1 Implementation Plan are no longer used, and therefore are not referenced in this Implementation Plan.

~~required to demonstrate compliance to these requirements by the *Compliant* milestone date in Table 2~~Implementation Plan.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC in April 2008 or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by the Responsibility Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsibility Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

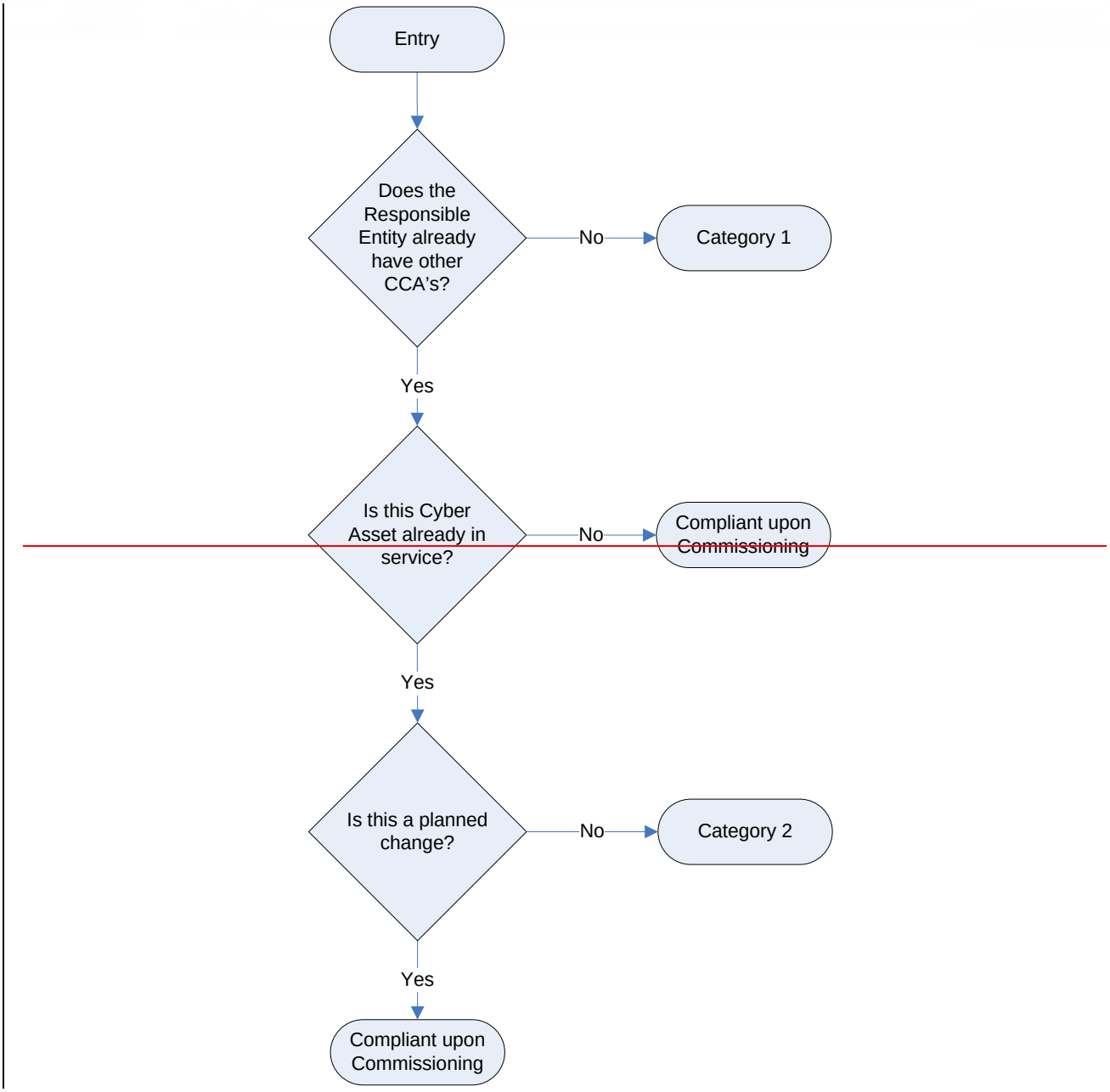
Note that the phrase ‘Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009’ as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation. (Compliant Upon Commisioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on established criteria or thresholds in the Responsible Entity's existing risk-based Critical Asset identification method (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of that risk-based Critical Asset Identification process is required annually (by CIP-002 R2), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.


Entry
Does the Responsible Entity already have other CCA's?
No
Category 1
Yes
Is this Cyber Asset already in service?
No
Compliant upon Commissioning
Yes
Is this a planned change?
No
Category 2
Yes
Compliant upon Commissioning

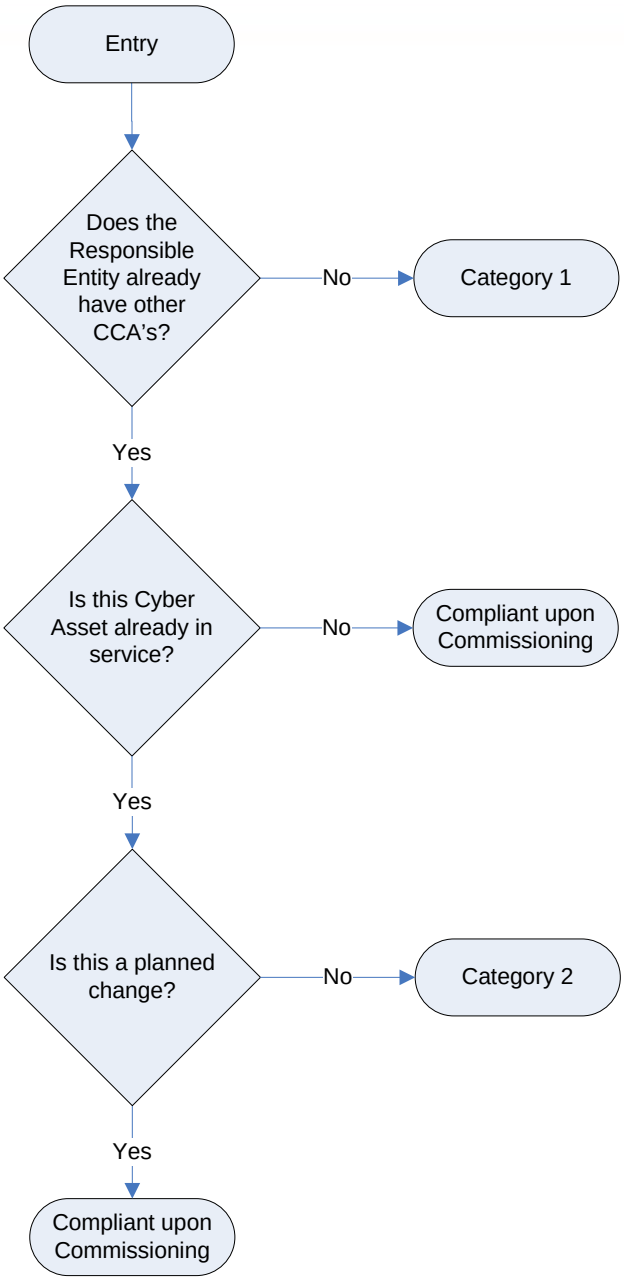


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on planning or impact studies) upon its commissioning or activation.
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset.
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset.
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to

demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 ~~Scenario:~~Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset

   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is the NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology implementation by each predecessor Responsible Entity.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate risk-based Critical Asset identification methodology implementation while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of risk-based Critical Asset identification methodology(ies) as required in CIP-002 R2, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate methodologies, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the risk-based Critical Asset identification methodology as required

in CIP-002 R2, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R3. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. ~~Category 2~~Newly Registered Entity Scenario 2:

A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology from Scenario 1 above would apply in this case as well.

3. Newly Registered Entity Scenario 3:

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing risk-based Critical Asset identification methodology and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as risk-based Critical Asset identification methodology. This scenario will be discussed in two sections, the first dealing with the combination of risk-based Critical Asset identification methodologies; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the risk-based Critical Asset identification methodologies: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate risk-based Critical Asset identification methodologies while determining how to either combine the risk-based

Critical Asset identification methodologies, or at a minimum, operate the separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined risk-based Critical Asset identification methodology and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R2 and R3. If additional Critical Assets are identified as a result of the application of the merged risk-based Critical Asset identification methodology, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan

for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merge plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated Critical Asset, but no newly designated Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5] Compliance Schedule for Standards CIP-002-2 through CIP-009-2 or CIP-002-3 through CIP-009-3 For Entities Registering in April 2008 and Thereafter		
	Registration + 12 months	Registration + 24 months
	All Facilities	All Facilities
CIP-002-2 or CIP-002-3 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-2 or CIP-003-3 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-2 or CIP-004-3 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-2 or CIP-005-3 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-2 or CIP-006-3 — Physical Security		
All Requirements		Compliant
Standard CIP-007-2 or CIP-007-3 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-2 or CIP-008-3 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-2 or CIP-009-3 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note — The requirement text in R1.6, R1.6.1, and R.1.6.2 for CIP-006-3 was updated. No changes were made to the VRFs.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 3 CIP-002-3 thru CIP-009-32 Standards:

Index:

Standard Number CIP-003 — Security Management Controls			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP–003–3	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.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	MEDIUM
CIP–006-3a	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:~~A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components:~~	MEDIUM
CIP–006-3a	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.~~Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.~~	MEDIUM
CIP–006-3a	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter~~Requirement for continuous escorted access within the Physical Security Perimeter of visitors.~~	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate	MEDIUM

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
		notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	LOWER

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition fromCIP-002-2 through CIP-009-2 to CIP-002-3 through CIP-009-3.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 3 CIP-002-3 thru CIP-009-32 Standards:

Index:

Standard Number CIP-003 — Security Management Controls			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP–003–~~2~~3	R2.3.	Where allowed by Standards CIP-002-3~~2~~ through CIP-009-~~2~~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.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~ 3 Requirement R4.	MEDIUM
CIP–006-3a~~CIP-006-2~~	R1.6~~R1.6.~~	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components:~~Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.~~	MEDIUM~~MEDIUM~~
CIP–006-3a	R1.6.1	Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.	MEDIUM
CIP–006-3a	R1.6.2	Requirement for continuous escorted access within the Physical Security Perimeter of visitors.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~ 3 Requirement R3; Standard CIP-005-~~2~~ 3 Requirements R2 and R3; Standard CIP-006-~~2~~ 3a Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-~~2~~3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
		least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.	

Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-2 through CIP-009-2 into CIP-002-3 through CIP-009-3.

Proposed Violation Severity Levels for the CIP Version 3 Series of Standards (Project 2009-21):

Index:

Standard Number CIP-005-3 — Electronic Security Perimeter(s)				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3, Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-33; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
R1.6. (V3 proposed)	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	The Responsible Entity did not include or implement a visitor control program in its physical security plan.
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3aRequirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	CIP-008-3; and Standard CIP-009-3.	3.	CIP-008-3; and Standard CIP-009-3.	Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
R5.	N/A	The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.	The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.	The Responsible Entity **has not documented nor implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
		• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-3.

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-3 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-003-3 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-003-3 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-003-3 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).
R5.1.3.	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-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
R7.	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-	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-005-3 **but** did not address	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-005-3 **but** did not address disposal as	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-

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	005-3 **but** did not maintain records as specified in R7.3.	redeployment as specified in R7.2.	specified in R7.1.	3.
R9.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 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-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-2 through CIP-009-2 into CIP-002-3 through CIP-009-3.

Proposed Violation Severity Levels for the CIP Version 3 Series of Standards (Project 2009-21):

Index:

Standard Number CIP-005-~~2~~ 3 — Electronic Security Perimeter(s)				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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-003-3~~2~~; Standard CIP-004-3~~2~~ Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a~~2~~ Requirements~~s~~ R3, Standard CIP-007-3~~2~~ Requirements R1 and R3 through R9;~~,~~ Standard CIP-008-3~~2~~; and Standard ~~CIP-009-2~~CIP-009-3.	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-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3;~~,~~ Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3; Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9;~~,~~ Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	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-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3; Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is ~~not~~ provided without four (4) or more of the protective measures as specified in Standard ~~CIP-003-2~~CIP-003-33; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3;~~,~~ Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3;~~,~~ Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9;~~,~~ Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with ~~CIP-004-2~~CIP-004-3 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with ~~CIP-004-2~~CIP-004-3 Requirement R4.
R1.6. (V3 proposed)~~R1.6.~~	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~N/A~~	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~N/A~~	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.~~N/A~~	The Responsible Entity did not include or implement a visitor control program in its physical security plan.~~The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.~~
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3;	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.
R5.	N/A	The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without	The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without	The Responsible Entity **has not documented nor implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with ~~CIP-008-2~~CIP-008-3.

Standard Number ~~CIP-007-2~~CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in ~~CIP-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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).
R5.1.3.	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-003-2~~CIP-003-3 Requirement R5 and Standard ~~CIP-004-2~~CIP-004-3 Requirement R4.
R7.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security	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	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	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security

Standard Number ~~CIP-007-2~~CIP-007-3 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Perimeter(s) as identified and documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not maintain records as specified in R7.3.	documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not address redeployment as specified in R7.2.	documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not address disposal as specified in R7.1.	Perimeter(s) as identified and documented in Standard ~~CIP-005-2~~CIP-005-3.
R9.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard ~~CIP-007-2~~CIP-007-3 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-007-2~~CIP-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Initial Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Project 2009-21: Cyber Security Ninety-day Response
The initial ballot for critical infrastructure protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3, a general implementation plan, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* ended on November 30, 2009.

Ballot Results
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 89.58%
Approval: 88.07%

Since at least one negative ballot included a comment, these results are not final. A second (or recirculation) ballot must be conducted. Ballot criteria are listed at the end of the announcement.

Next Steps
As part of the recirculation ballot process, the drafting team will draft and post responses to voter comments. Due to the shortened schedule for this project, the recirculation ballot will likely begin within the next week.

Project Background
The purpose of this project is to modify certain CIP Reliability Standards in response to the directives issued in the Federal Energy Regulatory Commission (FERC) September 30, 2009 Order approving version 2 of the CIP standards. Modifications must be filed within 90 days the order, and the Standards Committee authorized deviations from the standards development process to facilitate this schedule. The revised standards include associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).

Applicability of Standards in Project
Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

Standards Development Process

The *Reliability Standards Development Procedure* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria

Approval requires both a (1) quorum, which is established by at least 75 percent of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results

Ballot Name:	Project 2009-21 - Cyber Security Ninety-day Response _in
Ballot Period:	11/20/2009 - 11/30/2009
Ballot Type:	Initial
Total # Votes:	215
Total Ballot Pool:	240
Quorum:	**89.58 % The Quorum has been reached**
Weighted Segment Vote:	88.07 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	66	1	49	0.875	7	0.125	4	6
2 - Segment 2.	11	0.9	9	0.9	0	0	1	1
3 - Segment 3.	57	1	36	0.8	9	0.2	4	8
4 - Segment 4.	13	1	7	0.7	3	0.3	2	1
5 - Segment 5.	46	1	33	0.825	7	0.175	3	3
6 - Segment 6.	27	1	19	0.905	2	0.095	2	4
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	7	0.6	6	0.6	0	0	1	0
9 - Segment 9.	4	0.1	1	0.1	0	0	1	2
10 - Segment 10.	9	0.9	9	0.9	0	0	0	0
Totals	**240**	**7.5**	**169**	**6.605**	**28**	**0.895**	**18**	**25**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Abstain	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	View
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Avista Corp.	Scott Kinney	Affirmative	
1	Baltimore Gas & Electric Company	John J. Moraski	Negative	View
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	

1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	City Utilities of Springfield, Missouri	Jeff Knottek	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	E.ON U.S. LLC	Larry Monday	Negative	
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Abstain	
1	LG&E Energy Transmission Services	Bradley Young		
1	Long Island Power Authority	Jonathan Appelbaum	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Negative	View
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	PacifiCorp	Mark Sampson		
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Abstain	
1	SaskPower	Wayne Guttormson		
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Negative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	
1	Southwestern Power Administration	Gary W Cox	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Transmission Agency of Northern California	James W. Beck	Affirmative	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Jason L. Murray	Abstain	
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Jason L Marshall	Affirmative	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	

2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Negative	View
3	Allegheny Power	Bob Reeping		
3	Ameren Services	Mark Peters	Abstain	
3	American Electric Power	Raj Rana	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	View
3	City of Farmington	Linda R. Jacobson	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Leslie Sibert	Negative	View
3	Georgia System Operations Corporation	R Scott S. Barfield-McGinnis	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Negative	View
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory David Woessner		
3	Lakeland Electric	Mace Hunter		
3	Lincoln Electric System	Bruce Merrill	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Don Horsley	Negative	View
3	Muscatine Power & Water	John Bos	Negative	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson	Negative	View
3	Santee Cooper	Zack Dusenbury	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tri-State G & T Association Inc.	Janelle Marriott		
3	Wisconsin Electric Power Marketing	James R. Keller	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ricky Bittle	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	LaGen	Richard Comeaux	Abstain	

4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Abstain	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Calpine Corporation	Duncan Brown	Affirmative	
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consolidated Edison Co. of New York	Edwin E Thompson	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Dynegy	Greg Mason	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Lakeland Electric	Thomas J Trickey	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin	Negative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	Mark Aikens	Negative	View
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	PacifiCorp Energy	David Godfrey	Affirmative	
5	Portland General Electric Co.	Gary L Tingley		
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	RRI Energy	Thomas J. Bradish	Affirmative	
5	Sacramento Municipal Utility District	Bethany Wright	Negative	View
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	South California Edison Company	Ahmad Sanati	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones	Affirmative	
5	Southeastern Power Administration	Douglas Spencer	Abstain	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Negative	
5	Tennessee Valley Authority	Frank D Cuzzort	Affirmative	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	Abstain	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell		
6	Great River Energy	Donna Stephenson		
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	

6	Louisville Gas and Electric Co.	Daryn Barker	Negative	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	
6	Western Area Power Administration - UGP Marketing	John Stonebarger	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	Edward C Stein	Edward C Stein	Affirmative	
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Abstain	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
8	Wally Magda	Wally Magda	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
9	Oregon Public Utility Commission	Jerome Murray	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool Regional Entity	Stacy Dochoda	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Consideration of Comments on Initial Ballot — Cyber Security Ninety-day Response (Project 2009-21)

Summary Consideration: The initial ballot achieved a quorum and a weighted segment approval of 88.07%. There were 16 comments submitted with a negative ballot, and six comments submitted with an affirmative ballot. All of the comments received and the drafting team's consideration of those comments are shown below.

The comments mostly addressed changes made to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and the visitor control program in CIP-006. The drafting team considered the comments and responded with clarifications on the intent and scope of the changes made to the draft for the initial ballot. No changes were made to the standards and the implementation plans following the initial ballot.

Segment:	1
Organization:	American Transmission Company, LLC
Member:	Jason Shaver
Comment:	It is ATC's opinion that the 12 months provided in Table 2 for becoming compliant with CIP-006-2 and CIP-007-2 may not be arealistic time line, depending on the facility identified, and that the SDT should re-evaluate its proposal. ATC would prefer to see CIP-006 and CIP-007 align with CIP-004's implementation milestone. (CIP-004 allows for an 18 month implementation window) a. CIP-004 establishes the requirements for how entities will identify the training and access to Critical Cyber Assets located within a Physical Security Parameter. b. CIP-006 establishes the requirements for how entities will (Physically) protect it's Critical Cyber Assets. Specifically R2.1 states that entities have to protect from unauthorized physical access. In other words from individuals that have not been identified in CIP-004 as having access and training. c. CIP-007 establishes the requirements for how entities will (Cyber) protect it's Critical Cyber Assets. Specifically R3.2 states that entities have to detect and alert for attempts at or actual unauthorized access. i. Because these three standards do not align in terms of implementation milestone it seems that a situation could occur in which entities have both Physical and Cyber protection for their Critical Cyber Assets but necessary personnel may not have the access per CIP-004.

	We believe that the 18 months implementation milestone for CIP-004 is necessary but that both CIP-006 and CIP-007 need to align with CIP-004 in-order to avoid the situation we have identified. ATC suggest that the SDT update Table 2 to acknowledge that it applies to both Version 2 and Version 3 standards. (NOTE: Table 3 already contains an "or" statement) The version 2 standards will become mandatory and enforceable on April 1, 2010. The Version 3 standards state that they will become effective on the first day of the third calendar quarter after applicable regulatory approval. (Example: If these standards are approved by FERC anytime between January 1, 2010 and March 31 2010 then they will become effective on November 1, 2010.) Does the SDT agree with our understanding? The Version 3 implementation plan states that "When these standards (Version 3) become effective, all prior versions of these standards are retired". ATC is curious with the recent NERC filing (FERC Docket RM10-5) for an interpretation for CIP-007-2a. It is our understanding that the interpretation contained in CIP-007-2a was not incorporated in CIP-007-3. Will the interpretation contained in CIP-007-2a be appended to CIP-007-3 following FERC approval?
Response: Thank you for your comments. It is the drafting team's opinion that 12 months is a reasonable time frame for the implementation of CIP-006 and CIP-007 for entities that already have a CIP compliance program in place. The additional 6 months allowed for CIP-004 provides the time necessary for entities to complete the training and risk assessment for any additional personnel once these have been implemented. Entities can start performing the training and risk assessment concurrent with the implementation of CIP-005, CIP-006 and CIP-007. The compliance milestones did not change from Version 2 to Version 3, but the drafting team will address this issue as part of the Version 4 development. The posted Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities includes the following statement on Page 1, immediately following the title: "***This Implementation Plan applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.***" FERC approved interpretations are attached to the affected standard (in a similar way the interpretation for CIP-006 R1.1 was attached as Appendix 1 to CIP-006-3a).	
Segment:	1, 3
Organization:	Duke Energy Carolina
Member:	Douglas E. Hils, Henry Ernst-Jr
Comment:	Duke Energy appreciates the drafting team's efforts on the CIP standards and Implementation Plan. However, the Implementation Plan for newly identified Critical Cyber Assets is unnecessarily complex and should be simplified in

	a future revision. It forces entities to track compliance at the Critical Cyber Asset level; this means at the device level. For each new cyber asset to which the standards apply, we must determine the time of compliance by each requirement because the length of time allowed to meet compliance may vary by each requirement. This approach is un-necessarily complex and will result in a lot of record keeping for the entities with little actual enhancement to security. Anything that can be done to simplify the approached used would be of benefit.
Response: Thank you for your comment. There are many circumstances under which a particular Responsible Entity can have newly identified Critical Cyber Assets. The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities covers these many circumstances to provide for an implementation schedule that is fair for all circumstances while reducing the complexity as much as possible. The compliance milestones did not change from Version 2 to Version 3, but the drafting team will address this issue as part of the Version 4 development.	
Segment:	1; 3; 3; 3; 3
Organization:	Southern Company Services, Inc.; Georgia Power Company; Gulf Power Company; Mississippi Power; Alabama Power Company
Member:	Horace Stephen Williamson; Leslie Sibert; Gwen S Frazier; Don Horsley; Bobby Kerley
Comment:	The documentary evidence necessary to prove auditable compliance on every new CCA device at every point in time will likely prove to be unreasonably burdensome. Also the implementation plan is unreasonably complex and needs to be revamped. We need a straightforward way to maintain the CCA list along with a reasonable way to demonstrate that changes were appropriate, timely, and in compliance with standards. The current implementation plan does not lend itself to straightforward way of maintaining the CCA list.
Response: Thank you for your comment. There are many circumstances under which a particular Responsible Entity can have newly identified Critical Cyber Assets. The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities covers these many circumstances to provide for an implementation schedule that is fair for all circumstances while reducing the complexity as much as possible. The compliance milestones did not change from Version 2 to Version 3, but the drafting team will address this issue as part of the Version 4 development.	
Segment:	3

Organization:	Central Lincoln PUD
Member:	Steve Alexanderson
Comment:	NERC may find it difficult to achieve approval when so much is included in a single project. Central Lincoln finds the use of the word "milestone" used in the context of Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to be odd. The word is usually associated with multiple stones along a path to an ultimate destination, yet only one milestone is associated with each requirement in a category per Table 2. Could this be reworded better?
Response: Thank you for your comment. The definition of "milestone" in common dictionaries includes: "a significant point in development " (Merriam-Webster) and "an event or achievement that marks an important stage in a process" (MacMillan). In the opinion of the drafting team, this word conveys the intent in the document.	
Segment:	1; 5; 6
Organization:	Manitoba Hydro
Member:	Michelle Rheault; Mark Aikens; Daniel Prowse
Comment:	The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was significantly changed after approval by industry and the NERC BOT. The changes, pertaining to periodic requirements, were not directed by FERC in Order 706 or Order RD09-7-000, or through industry comments. The changes require that for a number of requirements, which were not specified by NERC, with "… a prescribed periodicity… the first occurrence of the recurring requirement must be completed by the Compliant milestone date…", which could advance the need to meet the requirements up to a year. This is not the general understanding of the industry, and was not the guidance provided in the NERC (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1. From the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 document provided with the Version 1 standards, "Compliant means that the entity meets the full intent of the requirements, and is beginning to maintain required "data", "documents", "logs", and "records". Auditably Compliant means that the entity meets the full intent of the requirements and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data", "documents", "logs", and "records"." Meeting the intent of the requirements means that the processes, procedures and infrastructure are in place to begin collecting data during the Auditably Compliant period. A quarterly review should not need to be conducted before the Compliant date; it is completed, at latest, at the end of the first quarter of the compliance period.

	The direction provided in the new Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is unclear and inconsistent, as some unspecified requirements with a prescribed periodicity must have their first periodic occurrence completed by the compliance date, while other unspecified periodic requirements can begin collection of their respective data by the compliance date. It is too late to introduce new compliance direction for standards whose initial compliance dates will have passed by the time the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is approved. We recommend the removal of the paragraph on Page 2 which begins "A number of the NERC Reliability Standard requirements include a prescribed periodicity …". With the removal of that paragraph, the following paragraphs in that section are unnecessary and should also be removed.
Response: Thank you for your comment. References to this interpretation of periodicity were removed from the document before we began the initial ballot.	

Segment:	1
Organization:	Baltimore Gas & Electric Company
Member:	John J. Moraski
Comment:	Clarification is needed on how to apply a visitor control program for PSPs that have been established at a cabinet level (e.g., CCAs, or equipment treated as a CCA per CIP requirements, are housed within a secured cabinet that is located within a data center, and they are the only CCAs within the data center. Access to the cabinet that houses the CCAs is controlled, and therefore the cabinet serves as the PSP for these cyber assets)?
Response: Thank you for your comment. The visitor control program applies to all Physical Security Perimeters. Implementation of the specific controls to satisfy the requirements of the visitor control program is left up to each Responsible Entity.	

Segment:	1; 3; 4; 5
Organization:	Sacramento Municipal Utility District
Member:	Tim Kelley; James Leigh-Kendall; Mike Ramirez; Bethany Wright
Comment:	Sacramento Municipal Utility District disagrees with the defined "continuous" escort of R1.6.2. In its strictest sense it requires not letting the visitor out of sight. As with other standards reasonableness must be applied to standard

	interpretations. This standard should not require visitor escort into a room that contains no CCAs and only a single access point to the room, i.e. bathroom or meeting room. Discretion should be permitted by the responsible person(s) providing the escort to such facilities.
Response: Thank you for your comment. The requirement for continuous escort applies to any defined Physical Security Perimeter. If the Physical Security Perimeter includes meeting rooms or rooms with no Critical Cyber Asset, then the Responsible Entity is required to meet the requirements for continuous escort for persons who do not have authorized unescorted access to the defined Physical Security Perimeter. Responsible Entities have flexibility in defining Physical Security Perimeters as long as all Critical Cyber Assets are within a Physical Security Perimeter. This requirement was not changed from the Version 2 standards.	
Segment:	4
Organization:	Public Utility District No. 1 of Snohomish County
Member:	John D. Martinsen
Comment:	The definition of “continuous” in its strictest sense may be interpreted as not letting the visitor out of sight. More work is needed to clarify this, since restrooms, or other facilities may be within the security parameter. This may be addressed by addressed by adding language regarding areas in the secure areas that have a single point of entry or exit.
Response: Thank you for your comment. The requirement for continuous escort applies to any defined Physical Security Perimeter. The Responsible Entity is required to meet the requirements for continuous escort for persons who do not have authorized unescorted access to the defined Physical Security Perimeter. Responsible Entities have flexibility in defining Physical Security Perimeters as long as all Critical Cyber Assets are within a Physical Security Perimeter. This requirement was not changed from the Version 2 standards.	
Segment:	3
Organization:	San Diego Gas & Electric
Member:	Scott Peterson

Comment:	SDG&E does not agree with the change under CIP-006 to require logging each time a visitor exits the PSP, especially since the visitors are escorted. SDG&E believes that logging each time a visitor enters and logging the visitor out at the end of the visit is sufficient.
Response: Thank you for your comment. The FERC directive in the order specifically included logging of exit.	
Segment:	5
Organization:	U.S. Bureau of Reclamation
Member:	Martin Bauer
Comment:	Unfortunately, the SDT revised the language in CIP 006 regarding the visitor control program from the earlier version. While we agree with the change in R 1.6.2, the change to R 1.6.1 reduced the clarity and watered down what was required to be included in the visitor program. This change eliminates the requirement to log the visitors identity as well as who performed the escort. The changes were only apparent by comparing the two documents (see below). The changes were made on the pretext that is was more consistent with the FERC order and in response to comments received. Since FERC cannot write standard and the comments reduced the clarity of the requirement, we would disagree that it was an appropriate change. A visitor management program that does not include identification of visitors (unique identifiers as characterized in V1/2) is not a visitor management program. If you cannot identify who was there, there is no point in logging anything.
Response: Thank you for your comment. Requirement R6 of CIP-006-3 specifically requires sufficient information to uniquely identify individuals and the time of access. R1.6.1 provides the additional minimum requirements for the logging of visitors. Responsible Entities can include any additional requirements in their specific Visitor Control Program.	
Segment:	2
Organization:	Midwest ISO, Inc.
Member:	Jason L Marshall
Comment:	We voted affirmative because we do not have any major issues with the content of the changes. However, we disagree with the need to violate the FERC approved NERC Reliability Standards Development Procedure by shortcircuiting the time line of the procedure. None of these changes are significant or even plug a reliability gap.

	Rather the changes are really clarifications of what is required by continous escorting in CIP-006-2 R1.6. In fact, visitor pass management is already required by CIP-006-2 R1.4. We object to rushing these changes through because it does not allow proper vetting of the changes and because it distracts scarce resources working on the next generation of CIP standards from that important job of improving cyber security. The Commission's 90-day timeline does not allow one to file an intervention, request for time extension or clarification with any reasonable expectation of a response before NERC must have their changes ready. Further, the 90-day timeline also does not allow the NERC standards drafting team to make changes based on industry comments or voting. Furhtermore, the scarce resources drafting the next generation of CIP standards are same resources that had to make these changes to the CIP standards and respond to industry comments. This only serves to delay the development of the true enhancements to the CIP standards by the amount of time it takes to develop these Commission ordered clarifying modifications.

Response: The drafting team appreciates your comment. As the ERO, NERC has an obligation to comply with the Commission's directives.

Segment:	5
Organization:	Northern States Power Co.
Member:	Liam Noailles
Comment:	We felt that the drafting team's response to our comment in the last ballot was very helpful and addressed our concern. However, no corresponding clarification was made to the interpretation. Interpretations should not introduce new ambiguity. We feel that it is the drafting team's responsibility to ensure that the issues relating to "potential sources" is clear in the interpretation and modifications should be made. One suggested way to clarify the interpretation is to add some of the language in the drafting team's response to our comment in the last ballot.

Response: Thank you for your comment. However, this comment is not relevant to the modifications made for the Cyber Security 90-day response.

Standards Announcement

Recirculation Ballot Window Open
December 3–14, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Project 2009-21: Cyber Security Ninety-day Response

A recirculation ballot window for critical infrastructure protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3, a general implementation plan, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* is now open **until 8 p.m. EST on December 14, 2009**.

Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Recirculation Ballot Process

The Standards Committee encourages all members of the ballot pool to review the consideration of comments submitted with the initial ballots. In the recirculation ballot, votes are counted by exception only — if a ballot pool member does not submit a revision to that member's original vote, the vote remains the same as in the first ballot. Members of the ballot pool may:

- Reconsider and change their vote from the first ballot.
- Vote in the second ballot even if they did not vote on the first ballot.
- Take no action if they do not want to change their original vote.

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

The purpose of this project is to modify certain CIP Reliability Standards in response to the directives issued in the Federal Energy Regulatory Commission (FERC) September 30, 2009 Order approving version 2 of the CIP standards. Modifications must be filed within 90 days the order, and the Standards Committee authorized deviations from the standards development process to facilitate this schedule. The revised standards include associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).

Project page: http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator

Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Final Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Project 2009-21: Cyber Security Ninety-day Response
The recirculation ballot for critical infrastructure protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3, a general implementation plan, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* ended December 14, 2009.

Ballot Results
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 93.33%
Approval: 85.55%

The ballot pool approved the standards and implementation plans. Ballot criteria details are listed at the end of the announcement.

Next Steps
The standards and implementation plans will be submitted to the NERC Board of Trustees for approval.

Project Background
The purpose of this project is to modify certain CIP Reliability Standards in response to the directives issued in the Federal Energy Regulatory Commission (FERC) September 30, 2009 Order approving version 2 of the CIP standards. Modifications must be filed within 90 days the order, and the Standards Committee authorized deviations from the standards development process to facilitate this schedule. The revised standards include associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).

Project page: http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

Applicability of Standards in Project
Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

Standards Development Process

The *Reliability Standards Development Procedure* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria

Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results

Ballot Name:	Project 2009-21 - Cyber Security Ninety-day Response _rc
Ballot Period:	12/3/2009 - 12/14/2009
Ballot Type:	recirculation
Total # Votes:	224
Total Ballot Pool:	240
Quorum:	**93.33 % The Quorum has been reached**
Weighted Segment Vote:	85.55 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	66	1	49	0.845	9	0.155	4	4
2 - Segment 2.	11	0.9	9	0.9	0	0	2	0
3 - Segment 3.	57	1	39	0.78	11	0.22	2	5
4 - Segment 4.	13	1	7	0.7	3	0.3	2	1
5 - Segment 5.	46	1	34	0.81	8	0.19	2	2
6 - Segment 6.	27	1	20	0.952	1	0.048	3	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	7	0.7	6	0.6	1	0.1	0	0
9 - Segment 9.	4	0.2	2	0.2	0	0	1	1
10 - Segment 10.	9	0.9	8	0.8	1	0.1	0	0
Totals	**240**	**7.7**	**174**	**6.587**	**34**	**1.113**	**16**	**16**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	View
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Avista Corp.	Scott Kinney	Affirmative	
1	Baltimore Gas & Electric Company	John J. Moraski	Negative	View
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	

1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy	Paul Rocha	Affirmative	
1	Central Maine Power Company	Brian Conroy	Affirmative	
1	City Utilities of Springfield, Missouri	Jeff Knottek	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	E.ON U.S. LLC	Larry Monday	Negative	
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Damon Holladay		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Albert Poire	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	Lakeland Electric	Larry E Watt	Abstain	
1	Lee County Electric Cooperative	John W Delucca	Abstain	
1	LG&E Energy Transmission Services	Bradley Young		
1	Long Island Power Authority	Jonathan Appelbaum	Affirmative	
1	Manitoba Hydro	Michelle Rheault	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Otter Tail Power Company	Lawrence R. Larson	Affirmative	
1	PacifiCorp	Mark Sampson	Negative	
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Affirmative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Abstain	
1	SaskPower	Wayne Guttormson		
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sierra Pacific Power Co.	Richard Salgo	Affirmative	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Negative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Negative	View
1	Southwestern Power Administration	Gary W Cox	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Transmission Agency of Northern California	James W. Beck	Affirmative	
1	Tri-State G & T Association Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Jason L. Murray	Abstain	
2	BC Transmission Corporation	Faramarz Amjadi	Affirmative	
2	California ISO	Greg Tillitson	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Independent Electricity System Operator	Kim Warren	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Abstain	View
2	Midwest ISO, Inc.	Jason L Marshall	Affirmative	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	

2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Negative	View
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	View
3	City of Farmington	Linda R. Jacobson	Affirmative	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy Services, Inc.	Matt Wolf	Affirmative	
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Leslie Sibert	Negative	View
3	Georgia System Operations Corporation	R Scott S. Barfield-McGinnis	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier	Negative	View
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory David Woessner	Affirmative	
3	Lakeland Electric	Mace Hunter		
3	Lincoln Electric System	Bruce Merrill	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Don Horsley	Negative	View
3	Muscatine Power & Water	John Bos	Negative	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	PacifiCorp	John Apperson	Negative	
3	PECO Energy an Exelon Co.	John J. McCawley	Affirmative	
3	Platte River Power Authority	Terry L Baker	Negative	View
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson	Negative	View
3	Santee Cooper	Zack Dusenbury	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tri-State G & T Association Inc.	Janelle Marriott		
3	Wisconsin Electric Power Marketing	James R. Keller	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ricky Bittle	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	LaGen	Richard Comeaux	Abstain	

4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Calpine Corporation	Duncan Brown	Negative	View
5	City of Tallahassee	Alan Gale	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Consolidated Edison Co. of New York	Edwin E Thompson	Affirmative	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Dynegy	Greg Mason	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Lakeland Electric	Thomas J Trickey	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Louisville Gas and Electric Co.	Charlie Martin	Negative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	Mark Aikens	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	Northern States Power Co.	Liam Noailles	Negative	View
5	Orlando Utilities Commission	Richard Kinas	Affirmative	
5	PacifiCorp Energy	David Godfrey	Negative	
5	Portland General Electric Co.	Gary L Tingley		
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	PSEG Power LLC	Thomas Piascik	Affirmative	
5	RRI Energy	Thomas J. Bradish	Affirmative	
5	Sacramento Municipal Utility District	Bethany Wright	Negative	View
5	Salt River Project	Glen Reeves	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	South California Edison Company	Ahmad Sanati	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones	Affirmative	
5	Southeastern Power Administration	Douglas Spencer	Abstain	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Negative	
5	Tennessee Valley Authority	Frank D Cuzzort	Affirmative	
5	Tri-State G & T Association Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	Abstain	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Chris Lyons	Abstain	
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell		
6	Great River Energy	Donna Stephenson		
6	Lakeland Electric	Paul Shipps	Abstain	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	

6	Louisville Gas and Electric Co.	Daryn Barker	Negative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson	Affirmative	
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	
6	Western Area Power Administration - UGP Marketing	John Stonebarger	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	Edward C Stein	Edward C Stein	Affirmative	
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
8	Wally Magda	Wally Magda	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Affirmative	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Negative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool Regional Entity	Stacy Dochoda	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

EXHIBIT 3

Standard Drafting Team Roster

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

Chairman	Jeri Domingo Brewer — Special Assistant, Mid-Pacific Region	U.S. Bureau of Reclamation 2800 Cottage Way Regional Director's Office MP-106 Sacramento, California 95825	(916) 978-5198 (916) 978-5005 Fx jbrewer@usbr.gov
	Robert Antonishen — Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@opg.com
	Jim Brenton, CISSP-ISSAP — Director, CIP Standards Development	Electric Reliability Council of Texas, Inc. 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ercot.com
	Doug Johnson — Operations Support Group	ComEd	(630) 691-4593 douglas.johnson@ComEd.com
	Brian McKay	Xcel Energy, Inc.	Brian.McKay@xcelenergy.com
	Gerard Adamski — Vice President and Director of Standards	NERC 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx gerry.adamski@nerc.net
	Howard L. Gugel — Standards Development Coordinator	NERC 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx howard.gugel@nerc.net
	Jackie Collett — Cyber Security Operations Engineer	Manitoba Hydro	(204) 360-7709 jcollett@hydro.mb.ca
	Jay S. Cribb — Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. — Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@southernco.com
	Joe Doetzl — Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@kcpl.com
	Sharon Edwards — Project Manager	Duke Energy 139 E. 4th Streets — 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@duke-energy.com
	Gerald S. Freese — Director, Enterprise Information Security	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com

	Philip Huff — Security Analyst	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
	Frank Kim — Director, Power System Information Technology	Hydro One Networks, Inc. 49 Sarjeant Drive Barrie, Ontario L4N 4V9	(705) 792-3033 frank.kim@hydroone.com
	Richard Kinas — Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
	John Lim, CISSP — Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place — Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
	David L. Norton — Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue — MS: L-MOB-17A New Orleans, Louisiana 70113	(504) 576-5469 (504) 576-5123 Fx dnorto1@entergy.com
	Christopher Peters — Vice President, Cybersecurity Solutions	ICF International 9108 Main St. Fairfax, Virginia 20110	703-934-3864 cpeters@icfi.com
	David S Revill — Group Lead, Electronic Maintenance	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@gatrans.com
	Scott Rosenberger — Director, IT Security and Compliance	Luminant Energy 500 North Akard Dallas, Texas 75201	(214) 875-8731 scott.rosenberger@luminant.com
	Kevin Sherlin — Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
	Jon Stanford — Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@bpa.gov
	Keith Stouffer — Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive — Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 Fx keith.stouffer@nist.gov
	John D. Varnell — Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 Fx jvarnell@tnsk.com

	William Winters — IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue — Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@aps.com
Consultant to NERC	Hal Beardall	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive — P.O. Box 3062777 Tallahassee, Florida 32310-4161	(850) 644-4945 (850) 644-4968 Fx hbeardall@fsu.edu
Consultant to NERC	Joseph Bucciero — President and Executive Consultant	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525	(267) 981-5445 joe.bucciero@gmail.com
Consultant to NERC	Robert M. Jones — Director Florida Conflict Resolution Consortium	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive Tallahassee, Florida 32310-4161	(850) 644-6320 (850) 644-4968 Fx rmjones@fsu.edu
Consultant to NERC	Stuart Langton, PhD — Senior Fellow	Florida State University 2010 Wild Lime Drive Sanibel, Florida 33957	(239) 395-9694 (239) 395-3230 Fx slangton@mindspring.com
NERC Staff	Tom Hofstetter — Regional Compliance Auditor	NERC 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx tom.hofstetter@nerc.net
NERC Staff	Roger Lampila — Regional Compliance Auditor	NERC 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx roger.lampila@nerc.net
NERC Staff	Scott R. Mix — Manager Infrastructure Security	NERC 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 Fx scott.mix@nerc.net
NERC Staff	David Taylor — Manager of Standards Development	NERC 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx david.taylor@nerc.net
NERC Staff	Todd Thompson — Compliance Investigator	NERC 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx todd.thompson@nerc.net

EXHIBIT 4a

Revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities Proposed for Approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records."

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of either Version 2 or Version 3 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the risk-based Critical Asset identification methodology. Upon a subsequent annual application of the risk-based Critical Asset identification method in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, and Version 3) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2', or '-3') will be applied to that particular reference.
[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

In all cases where a *Compliant* milestone is specified in Table 2 (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant'[4]) one year following the *Compliant* milestone listed in this Implementation Plan.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC in April 2008 or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

[4] The term 'Auditably Compliant' (AC) used in this Implementation Plan for newly identified Critical Cyber Assets and newly Registered Entities means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" [see (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1]. Since in all cases, the 'Auditably Compliant' dates are one calendar year following the 'Compliant' (C) date, the Auditably Compliant dates are not specified in this plan. The terms 'Begin Work' (BW) and 'Substantially Compliant' (SC) used in the Version 1 Implementation Plan are no longer used, and therefore are not referenced in this Implementation Plan.

compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by the Responsibility Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsibility Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commisioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on established criteria or thresholds in the Responsible Entity's existing risk-based Critical Asset identification method (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of that risk-based Critical Asset Identification process is required annually (by CIP-002 R2), and, as such, it may not be immediately apparent that that particular

transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

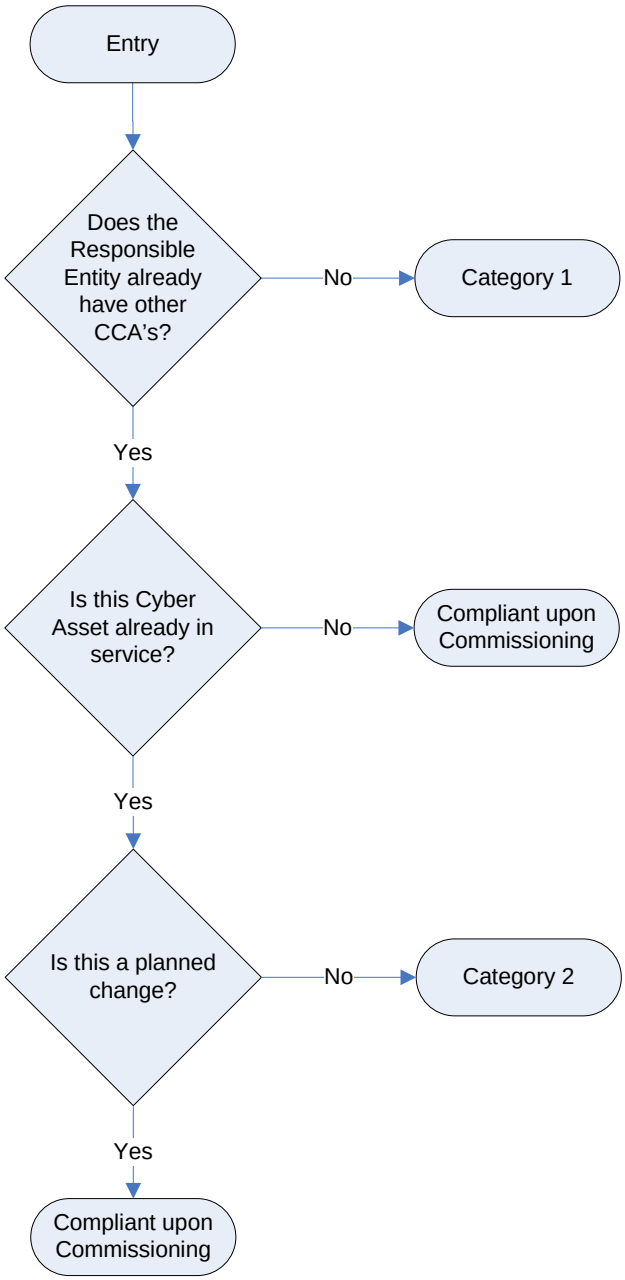


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on planning or impact studies) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to

demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002, and have existing risk-based Critical Asset identification methodologies.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is the NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology implementation by each predecessor Responsible Entity.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate risk-based Critical Asset identification methodology implementation while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this analysis, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of risk-based Critical Asset identification methodology(ies) as required in CIP-002 R2, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate methodologies, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the risk-based Critical Asset identification methodology as required in CIP-002 R2, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R3. If

newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

   Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 risk-based Critical Asset identification methodology from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

   A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing risk-based Critical Asset identification methodology and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as risk-based Critical Asset identification methodology. This scenario will be discussed in two sections, the first dealing with the combination of risk-based Critical Asset identification methodologies; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the risk-based Critical Asset identification methodologies: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate risk-based Critical Asset identification methodologies while determining how to either combine the risk-based Critical Asset identification methodologies, or at a minimum, operate the separate risk-based Critical Asset identification methodologies under a common Senior Manager and governance structure. It would be preferred that a single program be the result of this

analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined risk-based Critical Asset identification methodology and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R2 and R3. If additional Critical Assets are identified as a result of the application of the merged risk-based Critical Asset identification methodology, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merge plan' must be made

available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated Critical Asset, but no newly designated Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5] Compliance Schedule for Standards CIP-002-2 through CIP-009-2 or CIP-002-3 through CIP-009-3 For Entities Registering in April 2008 and Thereafter				
	Registration + 12 months	Registration + 24 months		
	All Facilities	All Facilities		
CIP-002-2 or CIP-002-3 — Critical Cyber Assets				
All Requirements		Compliant		
Standard CIP-003-2 or CIP-003-3 — Security Management Controls				
All Requirements Except R2		Compliant		
R2	Compliant			
Standard CIP-004-2 or CIP-004-3 — Personnel & Training				
All Requirements		Compliant		
Standard CIP-005-2 or CIP-005-3 — Electronic Security				
All Requirements		Compliant		
Standard CIP-006-2 or CIP-006-3 — Physical Security				
All Requirements		Compliant		
Standard CIP-007-2 or CIP-007-3 — Systems Security Management				
All Requirements		Compliant		
Standard CIP-008-2 or CIP-008-3 — Incident Reporting and Response Planning				
All Requirements		Compliant		
Standard CIP-009-2 or CIP-009-3 — Recovery Plans				
All Requirements		Compliant		

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

EXHIBIT 4b

Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–3 — Cyber Security — Critical Cyber Asset Identification
CIP–003–3 — Cyber Security — Security Management Controls
CIP–004–3 — Cyber Security — Personnel and Training
CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–3 — Cyber Security — Physical Security
CIP–007–3 — Cyber Security — Systems Security Management
CIP–008–3 — Cyber Security — Incident Reporting and Response Planning
CIP–009–3 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date

The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard.

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 3 of the NERC Cyber Security Standards CIP-002-3 to CIP-009-3.

Prior Version Implementation Plan Retirement

By December 31, 2009, CIP Version 1's Table 1, 2, and 3 Registered Entities that registered prior to December 31, 2007 will have reached the "Compliant" milestone for all CIP Version 1 Requirements. Timetables for reaching the "Auditably Compliant" milestone will still be in effect for these Entities going forward until said timetables expire. As such, when Table 3 Registered Entities reach the Auditably Compliant milestone on December 31, 2010, the Version 1 Implementation Plan is in practice retired. Table 4 of the CIP Version 1 Implementation Plan is applicable only for newly Registered Entities, and compliance milestones for newly Registered Entities is included in CIP Version 2's Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities effective on April 1, 2010. CIP Version 3 milestones, are effective after FERC approval.

EXHIBIT 5

Order No. 706 Directives with Associated Timelines

Order No. 706 - Directives

Paragraph	Text	Version[1]/Approach	Status
13	NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.	Versions 2, 3, 4, post-4 Standards Development	NERC will update its timeline for addressing Order No. 706 directives in its filings for Versions 3, 4, and post 4 of the project. Each version will include a new or revised Implementation Plan.
25	We direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	Version 4 Standards Development	The NERC drafting team is proceeding to incorporate a NIST-like approach in Version 4 of the project. This will begin with the categorization process proposed in CIP-002-4, and continue with the suite of security controls/requirements in the re-write of CIP-003 through CIP-009.
75	We direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards	Version 2 Standards Development	Complete. Version 2 filed in May, 2009 and approved by FERC on September 30, 2009.
89	We direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule	Versions 2, 3, 4, Post-4 Standards Development	NERC will update its timeline for addressing Order No. 706 directives in its filings for Versions 3, 4, and Post-4 of the project. Each version will include a new or revised Implementation Plan.

90	We direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009
96	We direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required	CMEP program and self-certifications	Starting in July 2008, NERC and the Regional Entities have conducted semi-annual self certifications of registered entities up to the point that they become auditably compliant. This practice will continue through December 31, 2010, when Table 3 entities are expected to become auditably compliant. Although Version 1 of the CIP standards will be superseded by Version 2 on April 1, 2010, the semi-annual self certification practice will continue through December 31, 2010 in accordance with the compliance milestones set out in the Version 1 implementation plan – with registered entities self certifying against the relevant Versions of the CIP standards for the particular portions of the self-certification period. As part of the self-certifications for January 2009, July 2009, and July 2010, NERC and the Regional Entities have solicited more detailed information about responsible entities' designation of specific types f critical assets and critical cyber assets. That data collection may continue to be a part of the semi-annual, self-certification, or it may be folded into data request process under Rule 1600 of NERC's Rules of Procedure.

97	We adopt our CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify	CMEP, self-certification process	Per Order No. 706, Regional Entities identified in the semi-annual, self-certification process responsible entities that were not able to self-certify that they had met the BW and SC milestones under the Version 1 implementation plans. The Regional Entities discussed those issues with the responsible entities informally on a case-by-case, and often developed informal mitigation plans to ensure that the responsible entities achieved their compliant and auditably compliant milestones on schedule. Regional Entities have been prosecuting violations where responsible entities have failed to meet the compliant and auditably compliant dates.
106	The Commission adopts the CIP NOPR proposals and directs NERC to modify the CIP Reliability Standards through the Reliability Standards development process to remove the first two Terms ["reasonable business judgment," and "acceptance of risk"], and develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception	Version 2 – Standards Development TFE Filing/Rules of Procedure	Both are complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009. NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009.
128	The Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.

138	The Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
150	The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
156	The Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
178	The Commission Directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009.
186	The Commission adopts its proposal in the CIP NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009.

192	The Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009
209	The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009
211	The Commission directs the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009
212	The practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009

218	we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009.
219	We direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive information.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009
220	We direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009. NERC will submit a report annually as described in the filing.
221	We direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009. NERC will submit the report as a non-public filing containing information to be protected from unauthorized disclosure.
222	We direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009

222	We direct the ERO to develop appropriate modifications, as discussed above.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009.
233	We direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission.	Ongoing discussions with Cyber Security Order 706 Standard Drafting Team members from U.S. Bureau of Reclamation, Bonneville Power Administration, National Institute of Standards and Technology; Development of Version 4	These discussions continue to take place as the drafting team has begun the substantive work to produce Version 4 of the CIP standards. The team has begun to shape the Version 4 standards to be NIST-like but will continue to evaluate the suite of security controls (requirements) for their appropriateness to apply to the Bulk Power System assets being protected. These determinations will largely decide the final product delivered in Version 4.
253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance … leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	Critical Infrastructure Protection Committee Standards Committee	CIPC approved its CIP-002-1 guidance document for identifying critical assets in September, 2009. The Standards Committee approved the document as a reference document for use in conjunction with CIP-002-1 in November, 2009.
254	Direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary] when developing the guidance.	Critical Infrastructure Protection Committee Standards Committee Version 4 – Standards Development	CIPC approved its CIP-002-1 guidance document for identifying critical assets in September, 2009 that address these topics in part. The Standards Committee approved the document as a reference document for use in conjunction with CIP-002-1 in November, 2009. Additional consideration for these items will take place in the development of the revised CIP-002-4.

255	We direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.	In Progress	NERC is providing reasonable guidance directly through its monitoring of CIP-002-1 implementation as denoted by Michael Assante's letter to the industry dated April 7, 2009 and through the Critical Infrastructure Protection Committee (CIPC) development of critical asset and critical cyber asset identification guidelines. NERC plans to use supplemental questionnaires during the CIP self certification process and is working with the Regional Entities for CIP-002 focused spot checks and audits to better understand how entities are determining whether their assets are critical to the bulk power system. NERC has provided entity training specifically focused on CIP-002 and has used the monitoring process to provide overall feedback to entities regarding critical asset identification. NERC believes the best way to properly identify assets for protection is to revise the CIP-002-3 standard to provide more deterministic criteria to properly identify assets that are critical to the bulk power system. This activity is currently in progress.
257	We direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Critical Infrastructure Protection Committee Standards Committee Version 4 – Standards Development	CIPC approved its CIP-002-1 guidance document for identifying critical assets in September, 2009 that address the topic in part. The Standards Committee approved the document as a reference document for use in conjunction with CIP-002-1 in November, 2009. Additional consideration for this item will take place in the development of the revised CIP-002-4.

272	The Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Critical Infrastructure Protection Committee Standards Committee Version 4 – Standards Development	CIPC approved its CIP-002-1 guidance document for identifying critical assets in September, 2009 that address this topic. The Standards Committee approved the document as a reference document for use in conjunction with CIP-002-1 in November, 2009. However, because data is largely not addressed in the Versions 1, 2, or proposed Version 3 of the CIP standards, it was not appropriate to provide guidance in the document. Additional consideration for this item will take place in the development of the revised CIP-003-4 through CIP-009-4.
272	The Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Critical Infrastructure Protection Committee Standards Committee Version 4 – Standards Development	CIPC approved its CIP-002-1 guidance document for identifying critical assets in September, 2009 that address this topic. The Standards Committee approved the document as a reference document for use in conjunction with CIP-002-1 in November, 2009. However, because data is largely not addressed in the Versions 1, 2, or proposed Version 3 of the CIP standards, it was not appropriate to provide guidance in the document. Additional consideration for this item will take place in the development of the revised CIP-003-4 through CIP-009-4.

282	The Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	Critical Infrastructure Protection Committee Standards Committee Version 4 – Standards Development	CIPC approved its CIP-002-1 guidance document for identifying critical assets in September, 2009 that address this topic in part. The Standards Committee approved the document as a reference document for use in conjunction with CIP-002-1 in November, 2009. The document does address the topic of misuse. Additionally, NERC's Chief Security officer provided a letter to industry dated April 7, 2009 that clearly raised the issue of misuse of assets as an important element in the determination of critical assets. Additional consideration for this item will take place in the development of the revised Version-4 to include a review of terms in the NERC Glossary.
285	We direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable – by testing and experience].	Version 4 – Standards Development	Will be considered as part of the revision to CIP-002.
294	The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.

294	The Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Addressed in alternate way in Version 4, CIP-002.	The standard drafting team is pursuing an alternate approach for CIP-002 that will provide a more deterministic method so that designations of critical assets are more clear and will not require an external review and approval. No longer will a critical asset list be necessary in this context.
329	The Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	No Longer Addressed in alternate way in Version 4, CIP-002.	The standard drafting team is pursuing an alternate approach for CIP-002 that will provide a more deterministic method so that designations of critical assets are more clear and will not require an external review and approval. No longer will a critical asset list be necessary in this context.
333	We direct the ERO, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009.
355	The Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address.	Guideline	The development of this guidance document is predicated on the availability of revised Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of guidance to address this directive will be assigned.

376	The Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
381	The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 4 – Standards Development Guidelines	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4. The development of guidance is predicated on the availability of revised Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of guidance to address this directive will be assigned.

412	The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.	Guideline	The development of guidance is predicated on the availability of revised Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of guidance to address this directive will be assigned.
431	The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
433	We direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.

435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
443	The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.

473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
476	We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commission's determinations above.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
496	The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter	Post Version 4	
502	The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.	Post Version 4	

502	The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Post Version 4 Guideline	The development of guidance is predicated on the availability of revised post-Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of additional guidance will be assessed.
503	The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures.	Post Version 4	
511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
526	The Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.

528	The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
541	We adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
542	The Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
544	The Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
544	We are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
547	We direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	Post Version 4 – Standards Development	.

560	The Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions.	TFE Filing/Rules of Procedure Modification	NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification on October 29, 2009. In developing the Technical Feasible Exception process that NERC filed with FERC as a Rule of Procedure modification on October 29, 2009, NERC determined that Technical Feasibility Exceptions are not needed for R1.1 of CIP-006-2, and R3.2 and R4.1 of CIP-007-2 because strict compliance could entail simply documenting compensating or alternative measures. Based on the language of the requirements, a Responsible Entity could be compliance with CIP-006 R1.1 for a particular critical cyber asset without having a six-wall border; with CIP-007, R3.2 without installing every security patch; and with CIP-007, R4.1 for a particular critical cyber asset without installing anti-virus or malware prevention tools.
572	The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets.	Post Version 4	
575	The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Post Version 4 Guideline	The development of guidance is predicated on the availability of revised post-Version 4 requirements that have yet to be developed. When the requirements have been largely determined the development of additional guidance will be assessed and if needed assigned

581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
597	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
600	Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility.	Version 2 – Standards Development TFE Filing/Rules of Procedure	Both are complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009. NERC developed a process for managing the Technical Feasibility Exception process that it filed with FERC as a Rule of Procedure modification in October, 2009
609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	Version 4 – Standards Development Guidelines	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4. The development of guidance is predicated on the availability of revised Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of additional guidance will be assessed and if needed assigned.

610	We direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
611	The Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.

619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	Version 2 – Standards Development TFE Filing/Rules of Procedure Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4. The acceptance of risk was removed in Version 2; Requirement R7 addressed in the TFE filing; and the remaining items are included in Version 4 considerations.
622	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.

622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 4 – Standards Development Guidelines	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4. The development of guidance is predicated on the availability of revised Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of additional guidance will be assessed and if needed assigned.
633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.

635	The Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
643	The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.	Post Version 4	
651	We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
660	The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. … we direct the ERO to develop and provide guidance on the term reportable incident.	Version 4 – Standards Development Guidelines	The development of guidance is predicated on the availability of revised Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of additional guidance will be assessed and if needed assigned.

661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced	Version 4 – Standards Development Guidelines	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4. The development of guidance is predicated on the availability of revised Version 4 requirements that have yet to be developed. When the requirements have been largely determined, the development of additional guidance will be assessed and if needed assigned.
673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
676	The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.

686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
706	The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.	Post Version 4	
710	Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report.	Post Version 4	

725	The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.	Post Version 4.	
731	The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans.	Version 2 Standards Development	Complete. Version 2 changes to the CIP standards were proposed by NERC in May, 2009 to address the items noted. Version 2 CIP standards were approved by FERC on September 30, 2009.
739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.
748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use.	Version 4 – Standards Development	Will be considered as part of the revision to CIP-003 through CIP-009 in the second part of Version 4.

757	Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations.	VRF Filing(s)	Complete. NERC filed 7/30/2008
759	Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.	VRF Filing(s)	Complete. NERC filed 7/30/2008
767	The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors.	VRF Filing(s)	Complete. NERC filed 7/30/2008.

EXHIBIT 6a

Proposed Violation Risk Factors and Violation Severity Levels for Modified Version 3 CIP Standard Requirements

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 3 CIP-002-3 thru CIP-009-32 Standards:

Index:

Standard Number CIP-003 — Security Management Controls			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP–003–3	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.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	MEDIUM
CIP–006-3a	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM
CIP–006-3a	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	MEDIUM
CIP–006-3a	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	LOWER

Note — this document shows all the VRFs for the two standards that have changes to their VRFs as a result of the modifications made to transition fromCIP-002-2 through CIP-009-2 to CIP-002-3 through CIP-009-3.

Proposed Violation Risk Factor Modifications Consistent with the Changes Proposed in the Version 3 CIP-002-3 thru CIP-009-3 Standards:

Index:

Standard Number CIP-003 — Security Management Controls			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP–003–~~2~~3	R2.3.	Where allowed by Standards CIP-002-3~~2~~ through CIP-009-~~2~~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.	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
CIP-006-2	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~2~~ 3 Requirement R4.	MEDIUM
CIP–006-3a~~CIP-006-2~~	R1.6~~R1.6.~~	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following components:~~Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.~~	MEDIUM~~MEDIUM~~
CIP–006-3a	R1.6.1	Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.	MEDIUM
CIP–006-3a	R1.6.2	Requirement for continuous escorted access within the Physical Security Perimeter of visitors.	MEDIUM
CIP-006-2	R2.2.	Be afforded the protective measures specified in Standard CIP-003-~~2~~3; Standard CIP-004-~~2~~ 3 Requirement R3; Standard CIP-005-~~2~~ 3 Requirements R2 and R3; Standard CIP-006-~~2~~ 3a Requirements R4 and R5; Standard CIP-007-~~2~~3; Standard CIP-008-~~2~~3; and Standard CIP-009-~~2~~3.	MEDIUM
CIP-006-2	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-~~2~~3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at	LOWER

Standard Number CIP-006 — Physical Security of Critical Cyber Assets			
Standard Number	**Requirement Number**	**Text of Requirement**	**Violation Risk Factor**
		least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~2~~3.	

Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-2 through CIP-009-2 into CIP-002-3 through CIP-009-3.

Proposed Violation Severity Levels for the CIP Version 3 Series of Standards (Project 2009-21):

Index:

Standard Number CIP-005-3 — Electronic Security Perimeter(s)				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3, Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	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-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is not provided without four (4) or more of the protective measures as specified in Standard CIP-003-33; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not-address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
R1.6. (V3 proposed)	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	The Responsible Entity did not include or implement a visitor control program in its physical security plan.
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5;	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3aRequirements R4 and R5; Standard CIP-007-3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5;	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	CIP-008-3; and Standard CIP-009-3.	Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
R5.	N/A	The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for	The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for	The Responsible Entity **has not documented nor implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

Standard Number CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
		response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-3.

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-3 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-003-3 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-003-3 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-003-3 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).
R5.1.3.	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-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
R7.	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	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-	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-	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

Standard Number CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	documented in Standard CIP-005-3 **but** did not maintain records as specified in R7.3.	3 **but** did not address redeployment as specified in R7.2.	3 **but** did not address disposal as specified in R7.1.	documented in Standard CIP-005-3.
R9.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 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-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note — This report shows only those VSLs that are associated with requirements that were modified when converting CIP-002-2 through CIP-009-2 into CIP-002-3 through CIP-009-3.

Proposed Violation Severity Levels for the CIP Version 3 Series of Standards (Project 2009-21):

Index:

Standard Number CIP-005-~~2~~ 3 — Electronic Security Perimeter(s)				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.5.	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-003-3~~2~~; Standard CIP-004-3~~2~~ Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a~~2~~ Requirements~~s~~ R3, Standard CIP-007-3~~2~~ Requirements R1 and R3 through R9;~~,~~ Standard CIP-008-3~~2~~; and Standard ~~CIP-009-2~~CIP-009-3.	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-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3;~~,~~ Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3; Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9;~~,~~ Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	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-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3; Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is ~~not~~ provided without four (4) or more of the protective measures as specified in Standard ~~CIP-003-2~~CIP-003-33; Standard ~~CIP-004-2~~CIP-004-3~~-~~ Requirement R3;~~,~~ Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements~~s~~ R3;~~,~~ Standard ~~CIP-007-2~~CIP-007-3~~-~~ Requirements R1 and R3 through R9;~~,~~ Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.5.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with ~~CIP-004-2~~CIP-004-3 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with ~~CIP-004-2~~CIP-004-3 Requirement R4.
R1.6. (V3 proposed)~~R1.6.~~	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~N/A~~	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~N/A~~	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.~~N/A~~	The Responsible Entity did not include or implement a visitor control program in its physical security plan.~~The Responsible Entity's physical security plan does not address the process for continuous escorted access within the physical security perimeter.~~
R2.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3;	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
	R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.	Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard ~~CIP-003-2~~CIP-003-3; Standard ~~CIP-004-2~~CIP-004-3 Requirement R3; Standard ~~CIP-005-2~~CIP-005-3 Requirements R2 and R3; Standard ~~CIP-006-2~~CIP-006-3a Requirements R4 and R5; Standard ~~CIP-007-2~~CIP-007-3; Standard ~~CIP-008-2~~CIP-008-3; and Standard ~~CIP-009-2~~CIP-009-3.
R5.	N/A	The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without	The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without	The Responsible Entity **has not documented nor implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must

Standard Number ~~CIP-006-2~~CIP-006-3a — Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with ~~CIP-008-2~~CIP-008-3.

Standard Number ~~CIP-007-2~~CIP-007-3 — Systems Security Management				
R#	**Lower VSL**	**Moderate VSL**	**High VSL**	**Severe VSL**
R3.	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in ~~CIP-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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-003-2~~CIP-003-3 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).
R5.1.3.	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-003-2~~CIP-003-3 Requirement R5 and Standard ~~CIP-004-2~~CIP-004-3 Requirement R4.
R7.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security	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	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	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security

Standard Number ~~CIP-007-2~~CIP-007-3 — Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Perimeter(s) as identified and documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not maintain records as specified in R7.3.	documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not address redeployment as specified in R7.2.	documented in Standard ~~CIP-005-2~~CIP-005-3 **but** did not address disposal as specified in R7.1.	Perimeter(s) as identified and documented in Standard ~~CIP-005-2~~CIP-005-3.
R9.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard ~~CIP-007-2~~CIP-007-3 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-007-2~~CIP-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

EXHIBIT 6b

Complete Listing of Violation Risk Factors and Violation Severity Levels for Version 3 CIP Standards

Date	Standard	Requirement	Change that was made
12/21/2009	**CIP-006-2**	**R7.**	**Modified text of requirement to match verison 3**
12/21/2009	**CIP-006-2**	**R5.**	**Modified text of requirement to match verison 3**
12/21/2009	**CIP-006-2**	**R2.2.**	**Modified text of requirement to match verison 3**
12/21/2009	**CIP–006-3a**	**R1.6.2**	**Added text of requirement to match verison 3**
12/21/2009	**CIP–006-3a**	**R1.6.1**	**Added text of requirement to match verison 3**
12/21/2009	**CIP–006-3a**	**R1.6**	**Modified text of requirement to match verison 3**
12/21/2009	**CIP-006-2**	**R1.5.**	**Modified text of requirement to match verison 3**
12/21/2009	**CIP–003–3**	**R2.3.**	**Modified text of requirement to match verison 3**
12/16/2009	CIP-003-2	R2, R2.1, R2.2, R2.3, R2.4	Added Violation Risk Factors
12/16/2009	CIP-006-2	R1, R1.1, R1.2, R1.3, R1.4, R1.5, R1.6, R1.7, R1.8, R2, R2.1, R2.2, R3, R4, R5, R6, R7, R8, R8.1, R8.2, and R8.3	Added Violation Risk Factors
12/16/2009	CIP-007-1	R5.3.3	Changed VRF from Lower to Medium
12/16/2009	CIP-007-1	R5.1	Changed VRF from Lower to Medium
12/16/2009	CIP-005-1	R1.5	Changed VRF from Lower to Medium
12/16/2009	CIP-003-1	R4.1	Changed VRF from Lower to Medium
12/16/2009	INT-005-2, INT-006-2, and INT-008-2	All requirements and subrequirements	Changed Version Number from -2 to -3
10/21/2009	IRO-001-1.1	R8	RSG entered in error on the VRF Matrix in the Applicability section has been removed.
8/21/2009	CIP-002-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
8/21/2009	CIP-003-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
8/21/2009	CIP-004-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
8/21/2009	CIP-005-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
8/21/2009	CIP-006-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
8/21/2009	CIP-007-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
8/21/2009	CIP-008-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
8/21/2009	CIP-009-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	COM-001-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. COM-001-1.1 has been approved and is effective.
6/25/2009	COM-001-1.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab

Date	Standard	Requirement	Change that was made
6/25/2009	IRO-001-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. IRO-001-1.1 has been approved and is effective.
6/25/2009	IRO-001-1.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	IRO-006-3	All requirements and subrequirements	Removed from FERC Approved Standard Tab. IRO-006-4 has been approved and is effective.
6/25/2009	IRO-006-4	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	MOD-006-0	All requirements and subrequirements	Removed from FERC Approved Standard Tab. MOD-006-0.1 has been approved and is effective.
6/25/2009	MOD-006-0.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	MOD-016-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. MOD-016-1.1 has been approved and is effective.
6/25/2009	MOD-016-1.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	MOD-017-0	All requirements and subrequirements	Removed from FERC Approved Standard Tab. MOD-017-0.1 has been approved and is effective.
6/25/2009	MOD-017-0.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	MOD-019-0	All requirements and subrequirements	Removed from FERC Approved Standard Tab. MOD-019-0.1 has been approved and is effective.
6/25/2009	MOD-019-0.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	TOP-005-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. TOP-005-1.1 has been approved and is effective.
6/25/2009	TOP-005-1.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	TPL-001-0	All requirements and subrequirements	Removed from FERC Approved Standard Tab. TPL-001-0.1 has been approved and is effective.
6/25/2009	TPL-001-0.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	VAR-002-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. VAR-002-1.1a has been approved and is effective.
6/25/2009	VAR-002-1.1a	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/25/2009	BAL-002-WECC-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on March 25, 2009
6/25/2009	FAC-501-WECC-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on February 9, 2009
6/25/2009	INT-005-3	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.

Date	Standard	Requirement	Change that was made
6/25/2009	INT-006-3	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	INT-008-3	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	IRO-006-WECC-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	PER-005-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	PRC-004-WECC-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	TOP-002-2a	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on March 5, 2009
6/25/2009	TOP-007-WECC-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on March 25, 2009
6/25/2009	TPL-002-0a	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on October 24, 2008
6/25/2009	TPL-003-0a	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on October 24, 2008
6/25/2009	MOD-001-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on August 29, 2008 - Standard still pending.
6/25/2009	MOD-004-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on November 21, 2008 - Standard still pending.
6/25/2009	MOD-008-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on August 29, 2008 - Standard still pending.
6/25/2009	MOD-028-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on August 29, 2008 - Standard still pending.
6/25/2009	MOD-029-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on August 29, 2008 - Standard still pending.
6/25/2009	MOD-030-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab. This standard was filed on March 6, 2009 - Standard still pending.
6/25/2009	PRC-STD-001-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	PRC-STD-003-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	PRC-STD-005-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	TOP-STD-007-0	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	VAR-STD-002a-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	VAR-STD-002b-a	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.

Date	Standard	Requirement	Change that was made
6/25/2009	EOP-001-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	IRO-002-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	IRO-005-3	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	IRO-008-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	IRO-009-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	IRO-010-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	TOP-003-1	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	TOP-005-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/25/2009	TOP-006-2	All requirements and subrequirements	Added to the Pending Regulatory Approval Tab.
6/24/2009	BAL-001-0	All requirements and subrequirements	Removed from FERC Approved Standard Tab. BAL-001-0.1a has been approved and is effective.
6/24/2009	BAL-001-0.1a	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/24/2009	BAL-003-0	All requirements and subrequirements	Removed from FERC Approved Standard Tab. BAL-003-0.1b has been approved and is effective.
6/24/2009	BAL-003-0.1b	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/24/2009	BAL-004-WECC-01	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/24/2009	BAL-005-0b	All requirements and subrequirements	Removed from FERC Approved Standard Tab. BAL-005-0.1b has been approved and is effective.
6/24/2009	BAL-005-0.1b	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/24/2009	BAL-006-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. BAL-006-1.1 has been approved and is effective.
6/24/2009	BAL-006-1.1	All requirements and subrequirements	Added to the FERC Approved Standards Tab
6/24/2009	CIP-002-1	R1.	Changed VRF from Lower to Medium
6/24/2009	CIP-002-1	R1.2.	Changed VRF from Lower to Medium
6/24/2009	CIP-002-1	R2.	Changed VRF from Lower to High
6/24/2009	CIP-002-1	R3.	Changed VRF from Lower to High
6/24/2009	CIP-002-1	R3.1.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-003-1	R1.	Changed VRF from Lower to Medium

Date	Standard	Requirement	Change that was made
6/24/2009	CIP-003-1	R2.	Changed VRF from Lower to Medium
6/24/2009	CIP-003-1	R4.1.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-003-1	R5.1.2.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-004-1	R2.1	Changed VRF from Lower to Medium
6/24/2009	CIP-004-1	R2.2	Changed VRF from Lower to Medium
6/24/2009	CIP-004-1	R2.2.2.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-004-1	R2.2.3.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-004-1	R3.	Changed VRF from Lower to Medium
6/24/2009	CIP-004-1	R4.2.	Changed VRF from Lower to Medium
6/24/2009	CIP-005-1	R1.5.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-007-1	R1.1.	Changed VRF from Lower to Medium
6/24/2009	CIP-007-1	R5.1.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-007-1	R5.3.3.	Changed VRF from Missing - to be added to Lower
6/24/2009	CIP-007-1	R7.	Changed VRF from Missing - to be added to Lower
5/18/2009	IRO-006-4.1	All requirements and subrequirements	Added to Pending Regulatory Approval Tab
5/18/2009	MOD-021-0.1	All requirements and subrequirements	Added to Pending Regulatory Approval Tab
5/18/2009	PER-001-0.1	All requirements and subrequirements	Added to Pending Regulatory Approval Tab
5/18/2009	TPL-006-0.1	All requirements and subrequirements	Added to Pending Regulatory Approval Tab
2/3/2009	IRO-005-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. IRO-005-2 has been approved and is effective.
2/3/2009	IRO-005-2	All requirements and subrequirements	Moved from Pending Regulatory Approval tab to FERC Approved Standards tab
2/3/2009	TOP-004-1	All requirements and subrequirements	Removed from FERC Approved Standard Tab. TOP-004-2 has been approved and is effective.
2/3/2009	TOP-004-2	All requirements and subrequirements	Added to the FERC Approved Standards Tab
12/22/2008	NUC-001-1	All requirements and subrequirements	Moved from Pending Regulatory Approval tab to FERC Approved Standards tab
12/12/2008	CIP-003-1	R4.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R1.1.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R1.2.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R1.3.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R1.4.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R2.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R2.4.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R3.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R3.1.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R3.2.	Changed the VRF from LOWER to MEDIUM

Date	Standard	Requirement	Change that was made
12/12/2008	CIP-005-1	R4.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R4.2.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R4.3.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R4.4.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-005-1	R4.5.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-006-1	R1.5.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-006-1	R6.1.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R2.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R2.3.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R4.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R4.1.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R4.2.	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R5.1.3	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R5.2.1	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R5.2.3	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R6.1	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R6.2	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R6.3	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R8.2	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R8.3	Changed the VRF from LOWER to MEDIUM
12/12/2008	CIP-007-1	R8.4	Changed the VRF from LOWER to MEDIUM
13-Sep-08	PRC-023-1	All requirements and subrequirements except for R1	Changed GP in Applicability section to GO
13-Sep-08	PRC-002-1	R5	Changed Applicability to RRO
13-Sep-08	PRC-003-1	R3	Changed Applicability to RRO
13-Sep-08	PRC-012-0	R1 and its subrequirements	Changed Applicability to RRO
13-Sep-08	PRC-013-0	R1 and its subrequirements	Changed Applicability to RRO
9/5/2008	COM-002-2	R2	Added BA and RC to Applicability section
9/5/2008	EOP-001-0	R2	Removed BA and RC from Applicability section
9/5/2008	EOP-002-2	R9	Removed LSE and RC from Applicability section
9/5/2008	EOP-005-1	R11.5	Removed BA from Applicability section
9/5/2008	IRO-001-1	R!	Removed RC from Applicability section
9/5/2008	IRO-005-1	R9	Removed BA, GOP and TOP from Applicability section
9/5/2008	IRO-005-1	R10	Removed BA from Applicability section
9/5/2008	IRO-005-1	R11	Removed BA from Applicability section
9/5/2008	MOD-016-1	R2	Removed PA from Applicqability section
9/5/2008	TOP-003-0	R1.2	Removed BA from Applicability section
9/5/2008	TOP-005-1	R1	Removed RC from Applicability section
9/5/2008	TOP-005-1	R3	Removed RC from Applicability section
9/5/2008	TOP-005-1	R4	Removed BA and TOP from Applicability section
9/5/2008	TOP-006-1	R1.1	Removed BA and TOP from Applicability section
9/5/2008	TOP-006-1	R1.2	Removed RC from Applicability section

Date	Standard	Requirement	Change that was made
9/5/2008	TOP-007-0	R1	Removed RC from Applicability section
9/5/2008	TOP-008-1	R3	Removed RC from Applicability section
9/5/2008	VAR-001-1	R6.1	Removed GOP from Applicability section
9/5/2008	VAR-001-1	R11	Removed GO from Applicability section
9/5/2008	VAR-002-1	R1	Removed TOP from Applicability section
9/5/2008	VAR-002-1	R2.1	Removed TOP from Applicability section
9/5/2008	VAR-002-1	R5	Removed TOP from Applicability section
9/5/2008	VAR-002-1	R5.1	Removed TOP from Applicability section
9/2/2008	INT-001-3	R.1 and R1.1.	Removed LSE from Applicability section
9/2/2008	INT-005-2	R1.1.	Removed BA and RC from Applicability section
9/2/2008	INT-006-2	R1.	Removed IA from Applicability section
9/2/2008	INT-008-2	R1.	Removed BA, PSE, and TSP from Applicability section
9/2/2008	INT-008-2	R1.1.1.	Removed BA from Applicability section
8/22/2008	CIP-002 through CIP-009		Added Violation Risk Factors
8/21/2008			added "Change History" tab in Worksheet
8/21/2008	INT-001-3 through INT-008-2		Added Violation Risk Factors

Complete Violation Severity Levels Matrix

Encompassing All Commission-Approved Reliability Standards

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-001-0.1a	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 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. ***See Standard for Formula.***	The Balancing Authority Area's value of CPS1 is less than 100% but greater than or equal to 95%.	The Balancing Authority Area's value of CPS1 is less than 95% but greater than or equal to 90%.	The Balancing Authority Area's value of CPS1 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS1 is less than 85%.
BAL-001-0.1a	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}. ***See Standard for Formula.***	The Balancing Authority Area's value of CPS2 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS2 is less than 85% but greater than or equal to 80%.	The Balancing Authority Area's value of CPS2 is less than 80% but greater than or equal to 75%.	The Balancing Authority Area's value of CPS2 is less than 75%.
BAL-001-0.1a	R3.	Each Balancing Authority providing Overlap Regulation Service shall evaluate	N/A	N/A	N/A	The Balancing Authority providing Overlap Regulation

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				Service failed to use a combined ACE and frequency bias.
BAL-001-0.1a	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).	N/A	N/A	N/A	The Balancing Authority receiving Overlap Regulation Service failed to ensure that control performance was being evaluated in a manner consistent with the calculation methodology as described in BAL-001-01 R3.
BAL-002-0	R1.	Each Balancing Authority shall have access to and/or operate Contingency Reserve to respond to Disturbances. Contingency Reserve may be supplied from generation, controllable load resources, or coordinated adjustments to Interchange Schedules.	N/A	N/A	N/A	The Balancing Authority does not have access to and/or operate Contingency Reserve to respond to Disturbances.
BAL-002-0	R1.1.	A Balancing Authority may elect to fulfill its Contingency Reserve obligations by participating as a member of a Reserve Sharing Group. In such cases, the Reserve Sharing Group shall have the	N/A	N/A	N/A	The Balancing Authority has elected to fulfill its Contingency Reserve obligations by participating as a member of a Reserve

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		same responsibilities and obligations as each Balancing Authority with respect to monitoring and meeting the requirements of Standard BAL-002.				Sharing Group and the Reserve Sharing Group has not provided the same responsibilities and obligations as required of the responsible entity with respect to monitoring and meeting the requirements of Standard BAL-002.
BAL-002-0	R2.	Each Regional Reliability Organization, sub-Regional Reliability Organization or Reserve Sharing Group shall specify its Contingency Reserve policies, including:	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 1 of the following sub-requirements.	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 2 or 3 of the following sub-requirements.	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 4 or 5 of the following sub-requirements.	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify all 6 of the following sub-requirements.
BAL-002-0	R2.1.	The minimum reserve requirement for the group.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the minimum reserve requirement for the group.
BAL-002-0	R2.2.	Its allocation among members.	N/A	N/A	N/A	The Regional Reliability Organization, sub-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Regional Reliability Organization, or Reserve Sharing Group has failed to specify the allocation of reserves among members.
BAL-002-0	R2.3.	The permissible mix of Operating Reserve – Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the permissible mix of Operating Reserve – Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.
BAL-002-0	R2.4.	The procedure for applying Contingency Reserve in practice.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to provide the procedure for applying Contingency Reserve in practice.
BAL-002-0	R2.5.	The limitations, if any, upon	N/A	N/A	N/A	The Regional

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the amount of interruptible load that may be included.				Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the limitations, if any, upon the amount of interruptible load that may be included.
BAL-002-0	R2.6.	The same portion of resource capacity (e.g., reserves from jointly owned generation) shall not be counted more than once as Contingency Reserve by multiple Balancing Authorities.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has allowed the same portion of resource capacity (e.g., reserves from jointly owned generation) to be counted more than once as Contingency Reserve by multiple Balancing Authorities.
BAL-002-0	R3.	Each Balancing Authority or Reserve Sharing Group shall activate sufficient Contingency Reserve to comply with the DCS.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than 100% but greater than or equal to 95%.	less than 95% but greater than or equal to 90%.	less than 90% but greater than or equal to 85%.	less than 85%.
BAL-002-0	R3.1.	As a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency. All Balancing Authorities and Reserve Sharing Groups shall review, no less frequently than annually, their probable contingencies to determine their prospective most severe single contingencies.	The Balancing Authority or Reserve Sharing Group failed to review their probable contingencies to determine their prospective most severe single contingencies annually.	N/A	N/A	The Balancing Authority or Reserve Sharing Group failed to carry at least enough Contingency Reserve to cover the most severe single contingency.
BAL-002-0	R4.	A Balancing Authority or Reserve Sharing Group shall meet the Disturbance Recovery Criterion within the Disturbance Recovery Period for 100% of Reportable Disturbances. The Disturbance Recovery Criterion is:	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 90% and less than 100% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 0% and less than or equal to 70% of Reportable Disturbances.
BAL-002-0	R4.1.	A Balancing Authority shall return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to zero. For negative initial ACE values just prior to the Disturbance, the Balancing Authority shall	N/A	N/A	N/A	The Balancing Authority failed to return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		return ACE to its pre-Disturbance value.				zero or for negative initial ACE values failed to return ACE to its pre-Disturbance value.
BAL-002-0	R4.2.	The default Disturbance Recovery Period is 15 minutes after the start of a Reportable Disturbance. This period may be adjusted to better suit the needs of an Interconnection based on analysis approved by the NERC Operating Committee.	N/A	N/A	N/A	N/A
BAL-002-0	R5.	Each Reserve Sharing Group shall comply with the DCS. A Reserve Sharing Group shall be considered in a Reportable Disturbance condition whenever a group member has experienced a Reportable Disturbance and calls for the activation of Contingency Reserves from one or more other group members. (If a group member has experienced a Reportable Disturbance but does not call for reserve activation from other members of the Reserve Sharing Group, then that member shall report as a single Balancing Authority.) Compliance may be demonstrated by either of the following two methods:	The Reserve Sharing Group met the DCS requirement for more than 90% and less than 100% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 0% and less than or equal to 70% of Reportable Disturbances.
BAL-002-0	R5.1.	The Reserve Sharing Group	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reviews group ACE (or equivalent) and demonstrates compliance to the DCS. To be in compliance, the group ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.				
BAL-002-0	R5.2.	The Reserve Sharing Group reviews each member's ACE in response to the activation of reserves. To be in compliance, a member's ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.	N/A	N/A	N/A	N/A
BAL-002-0	R6.	A Balancing Authority or Reserve Sharing Group shall fully restore its Contingency Reserves within the Contingency Reserve Restoration Period for its Interconnection.	The Balancing Authority or Reserve Sharing Group restored less than 100% but greater than 90% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 90% but greater than 80% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 80% but greater than or equal to 70% of its Contingency Reserve during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than 70% of its Contingency Reserves during the Contingency Reserve Restoration Period.
BAL-002-0	R6.1.	The Contingency Reserve	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Restoration Period begins at the end of the Disturbance Recovery Period.				
BAL-002-0	R6.2.	The default Contingency Reserve Restoration Period is 90 minutes. This period may be adjusted to better suit the reliability targets of the Interconnection based on analysis approved by the NERC Operating Committee.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R1.	Each Balancing Authority shall review its Frequency Bias Settings by January 1 of each year and recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.	N/A	N/A	The Balancing Authority reviewed its Frequency Bias Settings prior January 1, but failed to recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.	The Balancing Authority failed to review its Frequency Bias Settings prior to January 1, and failed to recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.
BAL-003-0.1b	R1.1.	The Balancing Authority may change its Frequency Bias Setting, and the method used to determine the setting, whenever any of the factors used to determine the current bias value change.	N/A	N/A	N/A	The Balancing Authority changed its Frequency Bias Setting by changing the method used to determine the setting, without any of the factors used to determine the current bias value changing.
BAL-003-0.1b	R1.2.	Each Balancing Authority shall report its Frequency Bias Setting, and method for	The Balancing Authority has not reported its method	The Balancing Authority has not reported its	The Balancing Authority has not reported its method	The Balancing Authority has failed to report as directed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		determining that setting, to the NERC Operating Committee.	for calculating frequency bias setting.	frequency bias setting.	for calculating frequency bias and has not reported its frequency bias setting.	by the requirement.
BAL-003-0.1b	R2.	Each Balancing Authority shall establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways:	N/A	N/A	N/A	The Balancing Authority established and maintained a Frequency Bias Setting that was less than, the Balancing Authority's Frequency Response.
BAL-003-0.1b	R2.1.	The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours.	N/A	N/A	N/A	The Balancing Authority determination of the fixed Frequency Bias value was not based on observations and averaging the Frequency Response from Disturbances during on-peak hours.
BAL-003-0.1b	R2.2.	The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by analyzing Frequency Response	N/A	N/A	N/A	The Balancing Authorities variable frequency bias maintained was not based on an analyses of Frequency Response as it varied with factors such as load, generation, governor

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		as it varies with factors such as load, generation, governor characteristics, and frequency.				characteristics, and frequency.
BAL-003-0.1b	R3.	Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.	N/A	N/A	N/A	The Balancing Authority did not operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, during periods when such operation would not have been adverse to system or Interconnection reliability.
BAL-003-0.1b	R4.	Balancing Authorities that use Dynamic Scheduling or Pseudo-ties for jointly owned units shall reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.	N/A	N/A	N/A	The Balancing Authority that used Dynamic Scheduling or Pseudo-ties for jointly owned units did not reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.
BAL-003-0.1b	R4.1.	Fixed schedules for Jointly Owned Units mandate that Balancing Authority (A) that contains the Jointly Owned Unit must incorporate the respective share of the unit governor droop response for any Balancing Authorities that	N/A	N/A	N/A	The Balancing Authority (A) that contained the Jointly Owned Unit with fixed schedules did not incorporate the respective share of the unit governor

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		have fixed schedules (B and C). See the diagram below.				droop response for any Balancing Authorities that have fixed schedules (B and C).
BAL-003-0.1b	R4.2.	The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit shall not include their share of the governor droop response in their Frequency Bias Setting. ***See Standard for Graphic***	N/A	N/A	N/A	The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit, included their share of the governor droop response in their Frequency Bias Setting.
BAL-003-0.1b	R5.	Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that served native load failed to have a monthly average Frequency Bias Setting that was at least 1% of the entities estimated yearly peak demand per 0.1 Hz change.
BAL-003-0.1b	R5.1.	Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that does not serve native load did not have a monthly average Frequency Bias Setting that was at least 1% of its estimated maximum generation level in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the coming year per 0.1 Hz change.
BAL-003-0.1b	R6.	A Balancing Authority that is performing Overlap Regulation Service shall increase its Frequency Bias Setting to match the frequency response of the entire area being controlled. A Balancing Authority shall not change its Frequency Bias Setting when performing Supplemental Regulation Service.	N/A	The Balancing Authority that was performing Overlap Regulation Service changed its Frequency Bias Setting while performing Supplemental Regulation Service.	The Balancing Authority that was performing Overlap Regulation Service failed to increase its Frequency Bias Setting to match the frequency response of the entire area being controlled.	N/A
BAL-004-0	R.3.2.	The Balancing Authority shall offset its Net Interchange Schedule (MW) by an amount equal to the computed bias contribution during a 0.02 Hertz Frequency Deviation (i.e. 20% of the Frequency Bias Setting).	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 0 to 25% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 25 to 50% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 50 to 75% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 75% or more of the time error corrections.
BAL-004-0	R1.	Only a Reliability Coordinator shall be eligible to act as Interconnection Time Monitor. A single Reliability Coordinator in each Interconnection shall be designated by the NERC Operating Committee to serve as Interconnection Time Monitor.	N/A	N/A	N/A	The responsible entity has designated more than one interconnection time monitor for a single interconnection.
BAL-004-0	R2.	The Interconnection Time Monitor shall monitor Time	N/A	N/A	N/A	The RC serving as the Interconnection

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Error and shall initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.				Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
BAL-004-0	R3.	Each Balancing Authority, when requested, shall participate in a Time Error Correction by one of the following methods:	The Balancing Authority participated in more than 75% and less than 100% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 50% and less than or equal to 75% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 25% and less than or equal to 50% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in less than or equal to 25% of requested Time Error Corrections for the calendar year.
BAL-004-0	R3.1.	The Balancing Authority shall offset its frequency schedule by 0.02 Hertz, leaving the Frequency Bias Setting normal; or	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 0 to 25% of the time error corrections for the year.	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 25 to 50% of the time error corrections for the year.	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 50 to 75% of the time error corrections for the year.	The Balancing Authority failed to offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 75% or more of the time error corrections for the year.
BAL-004-0	R4.	Any Reliability Coordinator in an Interconnection shall have the authority to request the Interconnection Time Monitor to terminate a Time Error Correction in progress, or a scheduled Time Error Correction that has not begun, for reliability considerations.	N/A	N/A	N/A	The RC serving as the Interconnection Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Procedure.
BAL-004-0	R4.1.	Balancing Authorities that have reliability concerns with the execution of a Time Error Correction shall notify their Reliability Coordinator and request the termination of a Time Error Correction in progress.	N/A	N/A	N/A	The Balancing Authority with reliability concerns failed to notify the Reliability Coordinator and request the termination of a Time Error Correction in progress.
BAL-005-0.1b	R1.	All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	N/A
BAL-005-0.1b	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.	N/A	N/A	N/A	The Generator Operator with generation facilities operating in an Interconnection failed to ensure that those generation facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.1b	R1.2.	Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are	N/A	N/A	N/A	The Transmission Operator with transmission facilities operating in an Interconnection

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		included within the metered boundaries of a Balancing Authority Area.				failed to ensure that those transmission facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.1b	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.	N/A	N/A	N/A	The Load-Serving Entity with load operating in an Interconnection failed to ensure that those loads were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.1b	R2.	Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.	N/A	N/A	N/A	The Balancing Authority failed to maintain Regulating Reserve that can be controlled by AGC to meet Control Performance Standard.
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to ensure adequate metering, communications, and control equipment was provided.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to notify the Host Balancing Authority for whom it is controlling if it was unable to provide the service, as well as any Intermediate Balancing Authorities.
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority receiving Regulation Service failed to ensure that back-up plans were in place to provide replacement Regulation Service.
BAL-005-0.1b	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	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its inability to calculate ACE.	The Balancing Authority failed to calculate ACE as specified in the requirement.	N/A	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its inability to calculate ACE and failed to use the ACE calculation specified in the requirement in its attempt to calculate ACE.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		it shall notify its Reliability Coordinator.				
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority failed to operate AGC continuously when there were no adverse impacts OR if their AGC was inoperative the Balancing Authority failed to use manual control to adjust generation to maintain the Net Scheduled Interchange.
BAL-005-0.1b	R8.	The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.	N/A	N/A	N/A	The Balancing Authority failed to ensure that data acquisition for and calculation of ACE occurred at least every six seconds.
BAL-005-0.1b	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%.	N/A	N/A		The Balancing Authority failed to provide redundant and independent frequency metering equipment that automatically activated upon detection of failure, such that the minimum availability was less

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						than 99.95%.
BAL-005-0.1b	R9.	The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Interchanged Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection chose to omit the Interchange Schedule related to the HVDC link from the ACE equation. but failed to model it as internal generation or load.
BAL-005-0.1b	R10.	The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority failed to include the effect of Ramp rates in the Scheduled Interchange values to calculate ACE.
BAL-005-0.1b	R12.	Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.	N/A	N/A	N/A	The Balancing Authority failed to include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority failed to ensure Tie Line MW metering was telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. OR The Balancing Authority failed to ensure that megawatt-hour data is telemetered or reported at the end of each hour.
BAL-005-	R12.2.	Balancing Authorities shall	N/A	N/A	N/A	The Balancing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
0.1b		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.				Authority failed to ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service were filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority failed to install common metering equipment where Dynamic Schedules or Pseudo-Ties were implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.
BAL-005-0.1b	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	N/A	N/A	N/A	The Balancing Authority failed to perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.				accuracy of its control equipment OR the Balancing Authority failed to adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.
BAL-005-0.1b	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.	N/A	N/A	N/A	The Balancing Authority failed to 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.
BAL-005-0.1b	R15.	The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing	N/A	N/A	The Balancing Authority failed to periodically test backup power supplies at the	The Balancing Authority failed to provide adequate and reliable backup power supplies to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.			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.	ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.
BAL-005-0.1b	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.	The Balancing Authority failed to collect coincident data to the greatest practical extent.	N/A	The Balancing Authority failed to flag missing or bad data for operator display and archival purposes.	The Balancing Authority failed to sample data at least at the same periodicity with which ACE is calculated.
BAL-005-0.1b	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: ***See Standard for Values***	N/A	N/A	N/A	The Balancing Authority failed to at least annually check and calibrate its time error and frequency devices against a common reference.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-006-1.1	R1.	Each Balancing Authority shall calculate and record hourly Inadvertent Interchange.	N/A	N/A	N/A	Each Balancing Authority failed to calculate and record hourly Inadvertent Interchange.
BAL-006-1.1	R2.	Each Balancing Authority shall include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. The Balancing Authority shall take into account interchange served by jointly owned generators.	N/A	N/A	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. OR Failed to take into account interchange served by jointly owned generators.	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. AND Failed to take into account interchange served by jointly owned generators.
BAL-006-1.1	R3.	Each Balancing Authority shall ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority failed to ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-006-1.1	R4.	Adjacent Balancing Authority Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign. Each Balancing Authority shall compute its Inadvertent Interchange based on the following:	The Balancing Authority failed to record Actual Net Interchange values that are equal but opposite in sign to its Adjacent Balancing Authorities.	The Balancing Authority failed to compute Inadvertent Interchange.	The Balancing Authority failed to operate to a common Net Interchange Schedule that is equal but opposite to its Adjacent Balancing Authorities.	N/A
BAL-006-1.1	R4.1.	Each Balancing Authority, by the end of the next business day, shall agree with its Adjacent Balancing Authorities to:	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net Interchanged Schedule. AND The hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-1.1	R4.1.1.	The hourly values of Net Interchange Schedule.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Interchanged Schedule.
BAL-006-1.1	R4.1.2.	The hourly integrated megawatt-hour values of Net Actual Interchange.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-1.1	R4.2.	Each Balancing Authority shall use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.	N/A	N/A	N/A	The Balancing Authority failed to use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.
BAL-006-1.1	R4.3.	A Balancing Authority shall make after-the-fact corrections to the agreed-to daily and monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). Changes or corrections based on non-reliability considerations shall not be	N/A	N/A	N/A	The Balancing Authority failed to make after-the-fact corrections to the agreed-to daily and monthly accounting data to reflect actual operating conditions or changes or corrections based on non-reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reflected in the Balancing Authority's Inadvertent Interchange. After-the-fact corrections to scheduled or actual values will not be accepted without agreement of the Adjacent Balancing Authority(ies).				considerations were reflected in the Balancing Authority's Inadvertent Interchange.
BAL-006-1.1	R5.	Adjacent Balancing Authorities that cannot mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month shall, for the purposes of dispute resolution, submit a report to their respective Regional Reliability Organization Survey Contact. The report shall describe the nature and the cause of the dispute as well as a process for correcting the discrepancy.	Adjacent Balancing Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities, submitted a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute but failed to provide a process for correcting the discrepancy.	Adjacent Balancing Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month, failed to submit a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute as well as a process for correcting the discrepancy.	N/A	N/A

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-001-1	R1.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	N/A	N/A	The responsible entity has procedures for the recognition of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection but does not have a procedure for making their operating personnel aware of said events.	The responsible entity failed to have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.
CIP-001-1	R2.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	N/A	N/A	The responsible entity has demonstrated the existence of a procedure to communicate information concerning sabotage events, but not all of the appropriate parties in the interconnection are identified.	The responsible entity failed to have a procedure for communicating information concerning sabotage events.
CIP-001-1	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and	N/A	The responsible entity has demonstrated the existence of a	The responsible entity has demonstrated the existence of a	The responsible entity failed to have a response guideline for reporting

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.		response guideline for reporting disturbances due to sabotage events, but the guideline did not list all of the appropriate personnel to contact.	response guideline for reporting disturbances due to sabotage events, including all of the appropriate personnel to contact, but the guideline was not available to its operating personnel.	disturbances due to sabotage events.
CIP-001-1	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	N/A	N/A	The responsible entity has established communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, but has not developed a reporting procedure.	The responsible entity failed to establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, nor developed a reporting procedure.
CIP-002-2	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)		of Critical Assets **or** the list of Critical Cyber Assets (even if such lists are null.)	methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-2	R2.	Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.	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 through CIP-009.
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
CIP-003-2	R2.3.	Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific	N/A	N/A	The identification of a senior manager's delegate does not include at least one of	A senior manager's delegate is not identified by name, title, and date of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.			the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	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 changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-2	R2.4.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	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.
CIP-003-2	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	**both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-004-2	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings,	The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		etc.).				
CIP-004-2	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, implement, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-2	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-2	R3.	Personnel Risk Assessment — The Responsible Entity shall	N/A	The Responsible Entity has a	The Responsible Entity has a	The Responsible Entity does not have

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.		personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
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 a specified in Standard CIP-003-2; Standard	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	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	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	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is ~~not~~ provided without four (4) or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	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-006-3a Requirements R3, Standard CIP-007-3 Requirements R1 and R3 through R9;~~,~~ Standard CIP-008-3; and Standard CIP-009-3.	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-006-3a Requirements~~s~~ R3; Standard CIP-007-3 Requirements R1 and R3 through R9;~~,~~ Standard CIP-008-3; and Standard CIP-009-3.	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-006-3a Requirements~~s~~ R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	more of the protective measures as specified in Standard CIP-003-33; Standard CIP-004-3 Requirement R3;~~,~~ Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements~~s~~ R3;~~,~~ Standard CIP-007-3 Requirements R1 and R3 through R9;~~,~~ Standard CIP-008-3; and Standard CIP-009-3.
CIP-005-2	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	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.
CIP-006-2	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum,	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).	The Responsible Entity did not document, implement, and maintain a physical security plan.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the following:			OR The Responsible Entity created and implemented but did not maintain a physical security plan.	
CIP-006-2	R1.1	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to ~~the Critical~~ such Cyber Assets within the Electronic Security Perimeter.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-2	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
CIP-006-2	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-3a	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-3a	R1.6.	Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	The Responsible Entity did not include or implement a visitor control program in its physical security plan.
CIP-006-2	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within-thirty calendar days of the completion of any physical security system redesign or reconfiguration **but** the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or reconfiguration.
CIP-006-2	R1.8.	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-3a	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3aRequirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Standard CIP-009-3.	Standard CIP-009-3.	Standard CIP-009-3.	point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
CIP-006-2	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
CIP-006-2	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to	N/A	The Responsible Entity **has implemented but not documented** the operational and procedural controls to	The Responsible Entity **has documented but not implemented** the operational and procedural controls to	The Responsible Entity has not documented nor implemented the operational and procedural controls to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other		manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring	manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring	manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		equivalent devices that control physical access to the Critical Cyber Assets.		station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-3a	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These	N/A	The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to	The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to	The Responsible Entity **has not documented nor implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.		personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-3.
CIP-006-2	R6.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	The Responsible Entity **has documented but not implemented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their	The Responsible Entity **has not implemented nor documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, **but** has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-2	R7.	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days.
CIP-006-2	R8.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
CIP-007-2	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.	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	The Responsible Entity **documented but did not establish (implement)** a process to ensure that only those ports and services required for normal and	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				emergency operations are enabled.	emergency operations are enabled.	emergency operations are enabled.
CIP-007-3	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-3 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-003-3 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-003-3 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-003-3 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).
CIP-007-2	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	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Entity shall document compensating measure(s) applied to mitigate risk exposure.				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.
CIP-007-3	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.	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-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
CIP-007-3	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	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Perimeter(s) as identified and documented in Standard CIP-005-2.	redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3 **but** did not maintain records as specified in R7.3.	Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3 **but** did not address redeployment as specified in R7.2.	Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3 **but** did not address disposal as specified in R7.1.	redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.
CIP-007-3	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 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-007-3 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.
CIP-008-2	R1.	Cyber Security Incident Response Plan — The	N/A	The Responsible Entity has developed	The Responsible Entity has developed	The Responsible Entity has not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:		but not maintained a Cyber Security Incident response plan.	a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.
CIP-009-2	R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the recovery plan(s) in more than 180 calendar days of the change.

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
COM-001-1.1	R1.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:	The responsible entity's telecommunications is not redundant or diversely routed as applicable by other operating entities for the exchange of interconnection or operating data.	The responsible entity's telecommunications is not redundant or diversely routed as applicable and has failed to establish telecommunications internally for the exchange of interconnection or operating data needed to maintain BES reliability.	The responsible entity's telecommunications is not redundant or diversely routed as applicable and has failed to establish telecommunications internally and with **other** Reliability Coordinators, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.	The responsible entity's telecommunications is not redundant or diversely routed as applicable and has failed to establish telecommunications internally and with both **other** and **its** Reliability Coordinators, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.1.	Internally.	N/A	N/A	N/A	The responsible entity has failed to establish telecommunications internally for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.2.	Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	The responsible entity has failed to establish telecommunications

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						with its Reliability Coordinator, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.3.	With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.	N/A	N/A	NA	The responsible entity has failed to establish telecommunications with other Reliability Coordinators, Transmission Operators, or Balancing Authorities for the exchange of interconnection or operating data needed to maintain BES reliability.
COM-001-1.1	R1.4.	Where applicable, these facilities shall be redundant and diversely routed.	N/A	N/A	N/A	The responsible entity's telecommunications is not redundant or diversely routed where applicable for the exchange of interconnection or operating data.
COM-001-1.1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall	N/A	The responsible entity has failed to manage, alarm, and	The responsible entity has failed to manage, alarm, and	The responsible entity has failed to manage, alarm, and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.		test or actively monitor its emergency telecommunications facilities.	test or actively monitor its primary telecommunications facilities.	test or actively monitor its primary and emergency telecommunications facilities.
COM-001-1.1	R3.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.	N/A	N/A	The responsible entity failed to assist in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.	The responsible entity failed to provide a means to coordinate telecommunications among their respective areas including assisting in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.
COM-001-1.1	R4.	Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing	N/A	N/A	N/A	If using a language other than English, the responsible entity failed to provide documentation of agreement to use a language other than English for all communications between and among operating personnel responsible for the real-time generation

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authorities may use an alternate language for internal operations.				control and operation of the interconnected Bulk Electric System.
COM-001-1.1	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.	N/A	N/A	N/A	The responsible entity did not have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.
COM-001-1.1	R6.	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, “NERCNet Security Policy.”	The NERCNet User Organization failed to adhere to less than 25% of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to 25% or more but less than 50% of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to 50% or more but less than 75% of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to 75% or more of the requirements listed in COM-001-0, Attachment 1, "NERCNet Security Policy".
COM-002-2	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.	N/A	The responsible entity did not have data links with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators.	The responsible entity did not staff the communications (voice and data links) on a 24 hour basis.	The responsible entity failed to have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators.
COM-002-2	R1.1.	Each Balancing Authority and	N/A	N/A	The responsible	The responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Operator shall notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.			entity failed to notify all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.	entity failed to notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.
COM-002-2	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall issue directives in a clear, concise, and definitive manner; shall ensure the recipient of the directive repeats the information back correctly; and shall acknowledge the response as correct or repeat the original statement to resolve any misunderstandings.	N/A	The responsible entity provided a clear directive in a clear, concise and definitive manner and required the recipient to repeat the directive, but did not acknowledge the recipient was correct in the repeated directive.	The responsible entity provided a clear directive in a clear, concise and definitive manner, but did not require the recipient to repeat the directive.	The responsible entity failed to provide a clear directive in a clear, concise and difinitive manner when required.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-001-0	R1.	Balancing Authorities shall have operating agreements with adjacent Balancing Authorities that shall, at a minimum, contain provisions for emergency assistance, including provisions to obtain emergency assistance from remote Balancing Authorities.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for less than 25% of the adjacent BAs. Or less than 25% of those agreements do not contain provisions for emergency assistance.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for 25% to 50% of the adjacent BAs. Or 25 to 50% of those agreements do not contain provisions for emergency assistance.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for 50% to 75% of the adjacent BAs. Or 50% to 75% of those agreements do not contain provisions for emergency assistance.	The Balancing Authority failed to demonstrate the existence of the necessary operating agreements for 75% or more of the adjacent BAs. Or more than 75% of those agreements do not contain provisions for emergency assistance.
EOP-001-0	R2.	The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. The plan shall include the details on how the Transmission Operator will implement load reduction in sufficient amount and time to mitigate the IROL violation before system separation or collapse would occur. The load reduction plan must be capable of being implemented within 30 minutes.	The Transmission Operator has demonstrated the existence of the emergency load reduction plan but the plan will take longer than 30 minutes.	N/A	The Transmission Operator fails to include details on how load reduction is to be implemented in sufficient amount and time to mitigate IROL violation.	The Transmission Operator failed to demonstrate the existence of emergency load reduction plans for all identified IROLs.
EOP-001-0	R3.	Each Transmission Operator and Balancing Authority shall:	The Transmission Operator or Balancing Authority failed to comply with one (1) of the sub-components.	The Transmission Operator or Balancing Authority failed to comply with two (2) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with three (3) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with four (4) of the sub-components.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-001-0	R3.1.	Develop, maintain, and implement a set of plans to mitigate operating emergencies for insufficient generating capacity.	The Transmission Operator or Balancing Authority's emergency plans to mitigate insufficient generating capacity are missing minor details or minor program/procedural elements.	The Transmission Operator or Balancing Authority's has demonstrated the existence of emergency plans to mitigate insufficient generating capacity emergency plans but the plans are not maintained.	The Transmission Operator or Balancing Authority's emergency plans to mitigate insufficient generating capacity emergency plans are not maintained nor implemented.	The Transmission Operator or Balancing Authority has failed to develop emergency mitigation plans for insufficient generating capacity.
EOP-001-0	R3.2.	Develop, maintain, and implement a set of plans to mitigate operating emergencies on the transmission system.	The Transmission Operator or Balancing Authority's plans to mitigate transmission system emergencies are missing minor details or minor program/procedural elements.	The Transmission Operator or Balancing Authority's has demonstrated the existence of transmission system emergency plans but are not maintained.	The Transmission Operator or Balancing Authority's transmission system emergency plans are not maintained nor implemented.	The Transmission Operator or Balancing Authority has failed to develop, maintain, and implement operating emergency mitigation plans for emergencies on the transmission system.
EOP-001-0	R3.3.	Develop, maintain, and implement a set of plans for load shedding.	The Transmission Operator or Balancing Authority's load shedding plans are missing minor details or minor program/procedural elements.	The Transmission Operator or Balancing Authority's has demonstrated the existence of load shedding plans but are not maintained.	The Transmission Operator or Balancing Authority's load shedding plans are partially compliant with the requirement but are not maintained nor implemented.	The Transmission Operator or Balancing Authority has failed to develop, maintain, and implement load shedding plans.
EOP-001-0	R3.4.	Develop, maintain, and implement a set of plans for	The Transmission Operator or	The Transmission Operator or	The Transmission Operator or	The Transmission Operator or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system restoration.	Balancing Authority's system restoration plans are missing minor details or minor program/procedural elements.	Balancing Authority's system restoration plans are partially compliant with the requirement but are not maintained.	Balancing Authority's restoration plans are not maintained nor implemented.	Balancing Authority has failed to develop, maintain, and implement operating emergency mitigation plans for system restoration.
EOP-001-0	R4.	Each Transmission Operator and Balancing Authority shall have emergency plans that will enable it to mitigate operating emergencies. At a minimum, Transmission Operator and Balancing Authority emergency plans shall include:	The Transmission Operator or Balancing Authority failed to comply with one (1) of the sub-components.	The Transmission Operator or Balancing Authority failed to comply with two (2) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with three (3) of the sub-components.	The Transmission Operator or Balancing Authority has failed to comply with all four (4) of the sub-components.
EOP-001-0	R4.1.	Communications protocols to be used during emergencies.	The Transmission Operator or Balancing Authority's communication protocols included in the emergency plan are missing minor program/procedural elements.	N/A	N/A	The Transmission Operator or Balancing Authority has failed to include communication protocols in its emergency plans to mitigate operating emergencies.
EOP-001-0	R4.2.	A list of controlling actions to resolve the emergency. Load reduction, in sufficient quantity to resolve the emergency within NERC-established timelines, shall be one of the controlling actions.	The Transmission Operator or Balancing Authority's list of controlling actions has resulted in meeting the intent of the requirement but is missing minor	N/A	The Transmission Operator or Balancing Authority provided a list of controlling actions; however the actions fail to resolve the emergency within NERC-established	The Transmission Operator or Balancing Authority has failed to provide a list of controlling actions to resolve the emergency.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			program/procedural elements.		timelines.	
EOP-001-0	R4.3.	The tasks to be coordinated with and among adjacent Transmission Operators and Balancing Authorities.	The Transmission Operator or Balancing Authority has demonstrated coordination with Transmission Operators and Balancing Authorities but is missing minor program/procedural elements.	N/A	N/A	The Transmission Operator or Balancing Authority has failed to demonstrate the tasks to be coordinated with adjacent Transmission Operator and Balancing Authorities as directed by the requirement.
EOP-001-0	R4.4.	Staffing levels for the emergency.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority's emergency plan does not include staffing levels for the emergency
EOP-001-0	R5.	Each Transmission Operator and Balancing Authority shall include the applicable elements in Attachment 1-EOP-001-0 when developing an emergency plan.	The Transmission Operator and Balancing Authority emergency plan has complied with 90% or more of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 70% to 90% of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with between 50% to 70% of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 50% or less of the number of sub-components
EOP-001-0	R6.	The Transmission Operator and Balancing Authority shall annually review and update each emergency plan. The	The Transmission Operator and Balancing Authority is missing minor	The Transmission Operator and Balancing Authority has failed to	The Transmission Operator and Balancing Authority has failed to	The Transmission Operator and Balancing Authority has failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Operator and Balancing Authority shall provide a copy of its updated emergency plans to its Reliability Coordinator and to neighboring Transmission Operators and Balancing Authorities.	program/procedural elements.	annually review one of it's emergency plans	annually review 2 of its emergency plans or communicate with 1 of its neighboring Balancing Authorities.	annually review and/or communicate any emergency plans with its Reliability Coordinator, neighboring Transmission Operators or Balancing Authorities.
EOP-001-0	R7.	The Transmission Operator and Balancing Authority shall coordinate its emergency plans with other Transmission Operators and Balancing Authorities as appropriate. This coordination includes the following steps, as applicable:	The Transmission Operator and/or the Balancing Authority failed to comply with one (1) of the sub-components.	The Transmission Operator and/or the Balancing Authority failed to comply with two (2) of the sub-components.	The Transmission Operator and/or the Balancing Authority has failed to comply with three (3) of the sub-components.	The Transmission Operator and/or the Balancing Authority has failed to comply with four (4) or more of the sub-components.
EOP-001-0	R7.1.	The Transmission Operator and Balancing Authority shall establish and maintain reliable communications between interconnected systems.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to establish and maintain reliable communication between interconnected systems.
EOP-001-0	R7.2.	The Transmission Operator and Balancing Authority shall arrange new interchange agreements to provide for emergency capacity or energy transfers if existing agreements cannot be used.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to arrange new interchange agreements to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						provide for emergency capacity or energy transfers with required entities when existing agreements could not be used.
EOP-001-0	R7.3.	The Transmission Operator and Balancing Authority shall coordinate transmission and generator maintenance schedules to maximize capacity or conserve the fuel in short supply. (This includes water for hydro generators.)	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to coordinate transmission and generator maintenance schedules to maximize capacity or conserve fuel in short supply.
EOP-001-0	R7.4.	The Transmission Operator and Balancing Authority shall arrange deliveries of electrical energy or fuel from remote systems through normal operating channels.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to arrange for deliveries of electrical energy or fuel from remote systems through normal operating channels.
EOP-002-2.1	R1.	Each Balancing Authority and Reliability Coordinator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area and shall exercise	N/A	N/A	N/A	The Balancing Authority or Reliability Coordinator does not have responsibility and clear decision-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		specific authority to alleviate capacity and energy emergencies.				making authority to take whatever actions are needed to ensure the reliability of its respective area OR The Balancing Authority or Reliability Coordinator did not exercise its authority to alleviate capacity and energy emergencies.
EOP-002-2.1	R2.	Each Balancing Authority shall implement its capacity and energy emergency plan, when required and as appropriate, to reduce risks to the interconnected system.	N/A	N/A	N/A	The Balancing Authority did not implement its capacity and energy emergency plan, when required and as appropriate, to reduce risks to the interconnected system.
EOP-002-2.1	R3.	A Balancing Authority that is experiencing an operating capacity or energy emergency shall communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.	N/A	N/A	The Balancing Authority communicated its current and future system conditions to its Reliability Coordinator but did not communicate to one or more of its neighboring Balancing Authorities.	The Balancing Authority has failed to communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-002-2.1	R4.	A Balancing Authority anticipating an operating capacity or energy emergency shall perform all actions necessary including bringing on all available generation, postponing equipment maintenance, scheduling interchange purchases in advance, and being prepared to reduce firm load.	N/A	N/A	N/A	The Balancing Authority has failed to perform the necessary actions as required and stated in the requirement.
EOP-002-2.1	R5.	A deficient Balancing Authority shall only use the assistance provided by the Interconnection's frequency bias for the time needed to implement corrective actions. The Balancing Authority shall not unilaterally adjust generation in an attempt to return Interconnection frequency to normal beyond that supplied through frequency bias action and Interchange Schedule changes. Such unilateral adjustment may overload transmission facilities.	N/A	N/A	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement corrective actions.	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement corrective actions and unilaterally adjust generation in an attempt to return Interconnection frequency to normal beyond that supplied through frequency bias action and Interchange Schedule changes.
EOP-002-2.1	R6.	If the Balancing Authority cannot comply with the Control Performance and Disturbance Control Standards, then it shall immediately implement remedies	The Balancing Authority failed to comply with one of the sub-components.	The Balancing Authority failed to comply with 2 of the sub-components.	The Balancing Authority failed to comply with 3 of the sub-components.	The Balancing Authority failed to comply with more than 3 of the sub-components.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to do so. These remedies include, but are not limited to:				
EOP-002-2.1	R6.1.	Loading all available generating capacity.	N/A	N/A	N/A	The Balancing Authority did not use all available generating capacity.
EOP-002-2.1	R6.2.	Deploying all available operating reserve	N/A	N/A	N/A	The Balancing Authority did not deploy all of its available operating reserve.
EOP-002-2.1	R6.3.	Interrupting interruptible load and exports.	N/A	N/A	N/A	The Balancing Authority did not interrupt interruptible load and exports.
EOP-002-2.1	R6.4.	Requesting emergency assistance from other Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority did not request emergency assistance from other Balancing Authorities.
EOP-002-2.1	R6.5.	Declaring an Energy Emergency through its Reliability Coordinator; and	N/A	N/A	N/A	The Balancing Authority did not declare an Energy Emergency through its Reliability Coordinator.
EOP-002-2.1	R6.6.	Reducing load, through procedures such as public appeals, voltage reductions, curtailing interruptible loads and firm loads.	N/A	N/A	N/A	The Balancing Authority did not implement one or more of the procedures stated in the requirement.
EOP-002-2.1	R7.	Once the Balancing Authority has exhausted the steps listed in	N/A	N/A	The Balancing Authority has met	The Balancing Authority has not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Requirement 6, or if these steps cannot be completed in sufficient time to resolve the emergency condition, the Balancing Authority shall:			only one of the two requirements	met either of the two requirements
EOP-002-2.1	R7.1.	Manually shed firm load without delay to return its ACE to zero; and	N/A	N/A	N/A	The Balancing Authority did not manually shed firm load without delay to return it's ACE to zero.
EOP-002-2.1	R7.2.	Request the Reliability Coordinator to declare an Energy Emergency Alert in accordance with Attachment 1-EOP-002-0 "Energy Emergency Alert Levels."	The Balancing Authority's implementation of an Energy Emergency Alert has missed minor program/procedural elements in Attachment 1-EOP-002-0.	N/A	N/A	The Balancing Authority has failed to meet one or more of the requirements of Attachment 1-EOP-002-0.
EOP-002-2.1	R8.	A Reliability Coordinator that has any Balancing Authority within its Reliability Coordinator area experiencing a potential or actual Energy Emergency shall initiate an Energy Emergency Alert as detailed in Attachment 1-EOP-002-0 "Energy Emergency Alert Levels." The Reliability Coordinator shall act to mitigate the emergency condition, including a request for emergency assistance if required.	The Reliability Coordinator's implementation of an Energy Emergency Alert has missed minor program/procedural elements in Attachment 1-EOP-002-0.	N/A	N/A	The Reliability Coordinator has failed to meet one or more of the requirements of Attachment 1-EOP-002-0.
EOP-002-2.1	R9.	When a Transmission Service Provider expects to elevate the	The Reliability Coordinator failed	The Reliability Coordinator failed	The Reliability Coordinator has	The Reliability Coordinator has

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources) as permitted in its transmission tariff (See Attachment 1-IRO-006-0 "Transmission Loading Relief Procedure" for explanation of Transmission Service Priorities):	to comply with one (1) of the sub-components.	to comply with two (2) of the sub-components.	failed to comply with three (3) of the sub-components.	failed to comply with all four (4) of the sub-components.
EOP-002-2.1	R9.1.	The deficient Load-Serving Entity shall request its Reliability Coordinator to initiate an Energy Emergency Alert in accordance with Attachment 1-EOP-002-0.	N/A	N/A	N/A	The Load-Serving Entity failed to request its Reliability Coordinator to initiate an Energy Emergency Alert.
EOP-002-2.1	R9.2.	The Reliability Coordinator shall submit the report to NERC for posting on the NERC Website, noting the expected total MW that may have its transmission service priority changed.	N/A	N/A	N/A	The Reliability Coordinator has failed to report to NERC as directed in the requirement.
EOP-002-2.1	R9.3.	The Reliability Coordinator shall use EEA 1 to forecast the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.	N/A	N/A	N/A	The Reliability Coordinator failed to use EEA 1 to forecast the change of the priority of transmission service as directed in the requirement.
EOP-002-	R9.4.	The Reliability Coordinator shall	N/A	N/A	N/A	The Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
2.1		use EEA 2 to announce the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.				Coordinator failed to use EEA 2 to announce the change of the priority of transmission service as directed in the requirement.
EOP-003-1	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed shed customer load.
EOP-003-1	R2.	Each Transmission Operator and Balancing Authority shall establish plans for automatic load shedding for underfrequency or undervoltage conditions.	N/A	N/A	N/A	The applicable entity did not establish plans for automatic load-shedding, as directed by the requirement.
EOP-003-1	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans among other interconnected Transmission Operators and Balancing Authorities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting 5% or less of its required entities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting between 5-10% of its required entities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting 10-15%, inclusive, of its required entities.	The applicable entity did not coordinate load shedding plans, as directed by the requirement, affecting greater than 15% of its required entities.
EOP-003-1	R4.	A Transmission Operator or Balancing Authority shall consider one or more of these	N/A	N/A	N/A	The applicable entity did not consider one of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		factors in designing an automatic load shedding scheme: frequency, rate of frequency decay, voltage level, rate of voltage decay, or power flow levels.				five required elements, as directed by the requirement.
EOP-003-1	R5.	A Transmission Operator or Balancing Authority shall implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority has failed to implement load shedding as directed in the requirement.
EOP-003-1	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority did not shed load.
EOP-003-1	R7.	The Transmission Operator and Balancing Authority shall coordinate automatic load shedding throughout their areas with underfrequency isolation of generating units, tripping of shunt capacitors, and other automatic actions that will occur under abnormal frequency, voltage, or power flow conditions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 5% or less of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting between 5 -10% of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 10-15%, inclusive, of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting greater than 15% of its automatic actions.
EOP-003-1	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator-controlled	N/A	The applicable entity did not have plans for operator	The applicable entity did not have the capability to	The applicable entity did not have plans for operator

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be capable of implementing the load shedding in a timeframe adequate for responding to the emergency.		controlled manual load shedding, as directed by the requirement.	implement the load shedding, as directed by the requirement.	controlled manual load shedding, as directed by the requirement nor had the capability to implement the load shedding, as directed by the requirement.
EOP-004-1	R1.	Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	The Regional Reliability Organization has demonstrated the existence of a regional reporting procedure, but the procedure is missing minor details or minor program/procedural elements.	The Regional Reliability Organization Regional reporting procedure have been is missing one element that would make the procedure meet the requirement.	The Regional Reliability Organization Regional has a regional reporting procedure but the procedure is not current.	The Regional Reliability Organization does not have a regional reporting procedure.
EOP-004-1	R2.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	N/A	The responsible entities has failed to analyze 1% to 25% of its disturbances on the BES or was negligent in the timeliness of analyzing the disturbances 1% to 25% of the time.	The responsible entities has failed to analyze 26% to 50% of its disturbances on the BES or was negligent in the timeliness of analyzing the disturbances 26% to 50% of the time.	The responsible entities has failed to analyze more than 50% of its disturbances on the BES or negligent in the timeliness of analyzing the disturbances more than 50% of the time
EOP-004-1	R3.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity	N/A	N/A	N/A	The responsible entities failed to provide a preliminary written

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.				report as directed by the requirement.
EOP-004-1	R3.1.	The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.		The responsible entities submitted the report within 25 to 36 hours of the disturbance or discovery of the disturbance.	The responsible entities submitted the report within 36 to 48 hours of the disturbance or discovery of the disturbance.	The responsible entities submitted the report more than 48 hours after the disturbance or discovery of the disturbance.
EOP-004-1	R3.2.	Applicable reporting forms are provided in Attachments 022-1 and 022-2.	N/A	N/A	N/A	N/A
EOP-004-1	R3.3.	Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission	The responsible entity provided its Reliability Coordinator and NERC with periodic, verbal updates about a disturbance, but the updates did not include all information that was	N/A	N/A	The responsible entity did not provide its Reliability Coordinator and NERC with verbal updates about a disturbance as specified in R3.3.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	available at the time.			
EOP-004-1	R3.4.	If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event.	The responsible entities final report is missing minor details or minor program/procedural elements.	The responsible entities final report was 30 days late or was missing one of the elements specified in the requirement.	The responsible entities final report was more than 30 days late or was missing two of the elements specified in the requirement.	The responsible entities final report was not submitted or was missing more than two of the elements specified in the requirement.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The report shall be subject to Regional Reliability Organization approval.				
EOP-004-1	R4.	When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	N/A	N/A	N/A	The RRO did not make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.
EOP-004-1	R5.	The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and	The Regional Reliability Organization reviewed all final report recommendations less than twice a year.	The Regional Reliability Organization reviewed 75% or more final report recommendations twice a year.	The Regional Reliability Organization has not reported on any recommendation has not been acted on within two years to the NERC Planning and Operating Committees.	The Regional Reliability Organization has not reviewed the final report recommendations or did not notify the NERC Planning and Operating Committees.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.				
EOP-005-1	R1.	Each Transmission Operator shall have a restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system, including necessary operating instructions and procedures to cover emergency conditions, and the loss of vital telecommunications channels. Each Transmission Operator shall include the applicable elements listed in Attachment 1-EOP-005 in developing a restoration plan.	The responsible entity has a restoration plan that includes 75 % or more but less than 100% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 50% to 75% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 25% - 50% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes less than 25% of the applicable elements listed in Attachment 1 OR the responsible entity has no restoration plan.
EOP-005-1	R2.	Each Transmission Operator shall review and update its restoration plan at least annually and whenever it makes changes in the power system network, and shall correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review or update its restoration plan when it made changes in the power system network.	The Transmission Operator failed to review and update its restoration plan at least annually.	The Transmission Operator failed to review and update its restoration plan at least annually or whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review and update its restoration plan at least annually and whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.
EOP-005-1	R3.	Each Transmission Operator shall develop restoration plans with a	N/A	N/A	N/A	The Transmission Operator's

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		priority of restoring the integrity of the Interconnection.				restoration plans failed to make restoration of the integrity of the Interconnection a top priority.
EOP-005-1	R4.	Each Transmission Operator shall coordinate its restoration plans with the Generator Owners and Balancing Authorities within its area, its Reliability Coordinator, and neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate its restoration plans with one of the entities listed in the requirement.	The Transmission Operator failed to coordinate its restoration plans with two of the entities listed in the requirement.	The Transmission Operator failed to coordinate its restoration plans with three of the entities listed in the requirement.	The Transmission Operator failed to coordinate its restoration plans with four or more of the entities listed in the requirement.
EOP-005-1	R5.	Each Transmission Operator and Balancing Authority shall periodically test its telecommunication facilities needed to implement the restoration plan.	N/A	N/A	N/A	The responsible entity failed to periodically test its telecommunication facilities needed to implement the restoration plan.
EOP-005-1	R6.	Each Transmission Operator and Balancing Authority shall train its operating personnel in the implementation of the restoration plan. Such training shall include simulated exercises, if practicable.	The responsible entity only trained less than 100% but greater than or equal to 67 % of its operating personnel in the implementation of the restoration plan.	The responsible entity only trained less than 67 % but greater than or equal to 33 % of its operating personnel in the implementation of the restoration plan.	The responsible entity only trained less than 33 % of its operating personnel in the implementation of the restoration plan.	The responsible entity did not trained any of its operating personnel in the implementation of the restoration plan.
EOP-005-1	R7.	Each Transmission Operator and Balancing Authority shall verify the restoration procedure by actual testing or by simulation.	The responsible entity verified 76% to 99% of the restoration procedure by actual testing or by	The responsible entity verified 51% to 75% of the restoration procedure by actual testing or by	The responsible entity verified 26% to 50% of the restoration procedure by actual testing or by	The responsible entity verified less than 26% of the restoration procedure by actual testing or by

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			simulation.	simulation.	simulation.	simulation.
EOP-005-1	R8.	Each Transmission Operator shall verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.	N/A	N/A	N/A	The Transmission Operator failed to verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.
EOP-005-1	R9.	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request. Such documentation may include Cranking Path diagrams.	N/A	N/A	N/A	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request.
EOP-005-1	R10.	The Transmission Operator shall demonstrate, through simulation	The Transmission Operator only	The Transmission Operator only	The Transmission Operator only	The Transmission Operator did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		or testing, that the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrated, through simulation or testing, that between 67 and 99% of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrated, through simulation or testing, that between 33 and 66% of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrated, through simulation or testing, that less than 33% of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	demonstrate, through simulation or testing, that any of the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.
EOP-005-1	R10.1.	The Transmission Operator shall perform this simulation or testing at least once every five years.	N/A	N/A	N/A	The Transmission Operator failed to perform the required simulation or testing at least once every five years.
EOP-005-1	R11.	Following a disturbance in which one or more areas of the Bulk Electric System become isolated or blacked out, the affected Transmission Operators and Balancing Authorities shall begin immediately to return the Bulk Electric System to normal.	The responsible entity failed to comply with less than 25% of the number of sub-components.	The responsible entity failed to comply with 25% or more and less than 50% of the number of sub-components.	The responsible entity failed to comply with 50% or more and less than 75% of the number of sub-components.	The responsible entity failed to comply with more than 75% of the number of sub-components.
EOP-005-1	R11.1.	The affected Transmission Operators and Balancing Authorities shall work in conjunction with their Reliability Coordinator(s) to determine the extent and condition of the isolated area(s).	N/A	N/A	N/A	The responsible entity failed to work in conjunction with their Reliability Coordinator to determine the extent and condition of the isolated area(s)
EOP-005-1	R11.2.	The affected Transmission	N/A	N/A	N/A	The affected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators and Balancing Authorities shall take the necessary actions to restore Bulk Electric System frequency to normal, including adjusting generation, placing additional generators on line, or load shedding.				Transmission Operators and Balancing Authorities failed to take the necessary actions to restore Bulk Electric System frequency to normal.
EOP-005-1	R11.3.	The affected Balancing Authorities, working with their Reliability Coordinator(s), shall immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments as needed to facilitate the restoration. The affected Balancing Authorities shall make all attempts to maintain the adjusted Interchange Schedules, whether generation control is manual or automatic.	N/A	N/A	The responsible entity failed to make all attempts to maintain adjusted Interchange Schedules as required in R11.3	The responsible entity failed to immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments to facilitate the restoration as required in R11.3.
EOP-005-1	R11.4.	The affected Transmission Operators shall give high priority to restoration of off-site power to nuclear stations.	N/A	N/A	N/A	The affected Transmission Operators failed to give high priority to restoration of off-site power to nuclear stations.
EOP-005-1	R11.5.	The affected Transmission Operators may resynchronize the isolated area(s) with the surrounding area(s) when the	The responsible entity failed to include one of the subrequirements.	The responsible entity failed to include two of the subrequirements.	The responsible entity failed to include three of the subrequirements.	The responsible entity failed to include four of the subrequirements.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		following conditions are met:				
EOP-005-1	R11.5.1.	Voltage, frequency, and phase angle permit.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-005-1	R11.5.2.	The size of the area being reconnected and the capacity of the transmission lines effecting the reconnection and the number of synchronizing points across the system are considered.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-005-1	R11.5.3.	Reliability Coordinator(s) and adjacent areas are notified and Reliability Coordinator approval is given.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-005-1	R11.5.4.	Load is shed in neighboring areas, if required, to permit successful interconnected system restoration.	N/A	N/A	N/A	The responsible entity failed to meet this requirement before resynchronizing isolated areas.
EOP-006-1	R1.	Each Reliability Coordinator shall be aware of the restoration plan of each Transmission Operator in its Reliability Coordinator Area in accordance with NERC and regional requirements.	The Reliability Coordinator is aware of more than 75% of its Transmission Operators restoration plans.	The Reliability Coordinator is aware of more than 50% but less than 75%of its Transmission Operators restoration plans.	The Reliability Coordinator is aware of more than 25% but less than 50% of its Transmission Operators restoration plans.	The Reliability Coordinator is not aware of any of its Transmission Operators restoration plans.
EOP-006-1	R2.	The Reliability Coordinator shall monitor restoration progress and coordinate any needed assistance.	N/A	N/A	The Reliability Coordinator failed to monitor	The Reliability Coordinator failed to monitor

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					restoration progress or failed to coordinate assistance.	restoration progress and failed to coordinate assistance.
EOP-006-1	R3.	The Reliability Coordinator shall have a Reliability Coordinator Area restoration plan that provides coordination between individual Transmission Operator restoration plans and that ensures reliability is maintained during system restoration events.	N/A	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not coordinate with one individual Transmission Operator restoration plans.	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not coordinate with more than one individual Transmission Operator restoration plans.	The Reliability Coordinator does not have a Reliability Coordinator Area restoration plan.
EOP-006-1	R4.	The Reliability Coordinator shall serve as the primary contact for disseminating information regarding restoration to neighboring Reliability Coordinators and Transmission Operators or Balancing Authorities not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to one neighboring Reliability Coordinator or Transmission Operator or Balancing Authority not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to two neighboring Reliability Coordinators or Transmission Operators or Balancing Authorities not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to three neighboring Reliability Coordinators or Transmission Operators or Balancing Authorities not immediately involved in restoration.	The Reliability Coordinator failed to disseminate information regarding restoration to four or more neighboring Reliability Coordinators or Transmission Operators or Balancing Authorities not immediately involved in restoration.
EOP-006-1	R5.	Reliability Coordinators shall approve, communicate, and coordinate the re-synchronizing of major system islands or synchronizing points so as not to	N/A	N/A	N/A	The Reliability Coordinators failed to approve, communicate, and coordinate the re-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cause a Burden on adjacent Transmission Operator, Balancing Authority, or Reliability Coordinator Areas.				synchronizing of major system islands or synchronizing points and caused a Burden on adjacent Transmission Operator, Balancing Authority, or Reliability Coordinator Areas.
EOP-006-1	R6.	The Reliability Coordinator shall take actions to restore normal operations once an operating emergency has been mitigated in accordance with its restoration plan.	N/A	N/A	N/A	The Reliability Coordinator failed to take actions to restore normal operations once an operating emergency has been mitigated in accordance with its restoration plan.
EOP-008-0	R1.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have a plan to continue reliability operations in the event its control center becomes inoperable. The contingency plan must meet the following requirements:	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with one of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with two of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with three or four of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with more than four of the sub-requirements.
EOP-008-0	R1.1.	The contingency plan shall not rely on data or voice communication from the primary control facility to be viable.	The responsible entity's contingency plan relies on data or voice communication from the primary	The responsible entity's contingency plan relies on data or voice communication from the primary	The responsible entity's contingency plan relies on data or voice communication from the primary	The responsible entity's contingency plan relies on data and voice communication from the primary

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			control facility for up to 25% of the functions identified in R1.2 and R1.3.	control facility for 25% to 50% of the functions identified in R1.2 and R1.3.	control facility for 50% to 75% of the functions identified in R1.2 and R1.3.	control facility for more than 75% of the functions identified in R1.2 and R1.3.
EOP-008-0	R1.2.	The plan shall include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.
EOP-008-0	R1.3.	The contingency plan must address monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events. The plan shall list the critical facilities.	The responsible entity's contingency plan failed to address one of the elements listed in the requirement.	The responsible entity's contingency plan failed to address two of the elements listed in the requirement.	The responsible entity's contingency plan failed to address three of the elements listed in the requirement.	The responsible entity's contingency plan failed to address four or more of the elements listed in the requirement.
EOP-008-0	R1.4.	The plan shall include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for maintaining basic voice

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						communication capabilities with other areas.
EOP-008-0	R1.5.	The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.
EOP-008-0	R1.6.	The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.
EOP-008-0	R1.7.	The plan shall be reviewed and updated annually.	The responsible entity’s plan was reviewed within 3 months of passing its annual review date.	The responsible entity’s plan was reviewed within 6 months of passing its annual review date.	The responsible entity’s plan was reviewed within 9 months of passing its annual review date.	The responsible entity’s plan was reviewed more than 9 months of passing its annual review date.
EOP-008-0	R1.8.	Interim provisions must be included if it is expected to take more than one hour to implement the contingency plan for loss of primary control facility.	N/A	N/A	N/A	The responsible entity failed to make interim provisions when it is took more than one hour to implement the contingency plan for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						loss of primary control facility.
EOP-009-0	R1.	The Generator Operator of each blackstart generating unit shall test the startup and operation of each system blackstart generating unit identified in the BCP as required in the Regional BCP (Reliability Standard EOP-007-0_R1). Testing records shall include the dates of the tests, the duration of the tests, and an indication of whether the tests met Regional BCP requirements.	The Generator Operator Blackstart unit testing and recording is missing minor program/procedural elements.	Startup and testing of each Blackstart unit was performed, but the testing records are incomplete. The testing records are missing 25% or less of data requested in the requirement'.	The Generator Operator's failed to test 25% or less of the Blackstart units or testing records are incomplete. The testing records are missing between 25% and 50% of data requested in the requirement.	The Generator Operator failed to test more than 25% of its Blackstart units or does not have Blackstart testing records or is missing more than 50% of the required data.
EOP-009-0	R2.	The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.	The Generator Operator has provided the Blackstart testing documentation to its Regional Reliability Organization. However the documentation provided had missing minor program/procedural elements or failed to provide the documentation requested to NERC in 30 days.	N/A	N/A	The Generator Operator did not provide the required Blackstart documentation to its Regional Reliability Organization.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R1.	The Transmission Owner shall document, maintain, and publish facility connection requirements to ensure compliance with NERC Reliability Standards and applicable Regional Reliability Organization, subregional, Power Pool, and individual Transmission Owner planning criteria and facility connection requirements. The Transmission Owner's facility connection requirements shall address connection requirements for:	Not Applicable.	The Transmission Owner's facility connection requirements failed to address connection requirements for one of the subrequirements.	The Transmission Owner's facility connection requirements failed to address connection requirements for two of the subrequirements.	The Transmission Owner's facility connection requirements failed to address connection requirements for three of the subrequirements.
FAC-001-0	R1.1.	Generation facilities,	The Transmission Owner has Generation facility connection requirements, but they have not been updated to include changes that are currently in effect, but have not been in effect for more than one month.	The Transmission Owner has Generation facility connection requirements, but they have not been updated to include changes that were effective more than one month ago, but not more than six months ago.	The Transmission Owner has Generation facility connection requirements, but they have not been updated to include changes that were effective more than six months ago.	The Transmission Owner does not have Generation facility connection requirements.
FAC-001-0	R1.2.	Transmission facilities, and	The Transmission Owner has Transmission facility connection requirements, but they have not been updated to include changes that are currently in effect,	The Transmission Owner has Transmission facility connection requirements, but they have not been updated to include changes that were effective more than	The Transmission Owner has Transmission facility connection requirements, but they have not been updated to include changes that were effective more than	The Transmission Owner does not have Transmission facility connection requirements.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			but have not been in effect for more than one month.	one month ago, but not more than six months ago.	six months ago.	
FAC-001-0	R1.3.	End-user facilities	The Transmission Owner has End-user facility connection requirements, but they have not been updated to include changes that are currently in effect, but have not been in effect for more than one month.	The Transmission Owner has End-user facility connection requirements, but they have not been updated to include changes that were effective more than one month ago, but not more than six months ago.	The Transmission Owner has End-user facility connection requirements, but they have not been updated to include changes that were effective more than six months ago.	The Transmission Owner does not have End-user facility connection requirements.
FAC-001-0	R2.	The Transmission Owner's facility connection requirements shall address, but are not limited to, the following items:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.1.	Procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.2.	Procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.3.	Voltage level and MW and MVAR capacity or demand at point of connection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.4.	Breaker duty and surge protection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						systems failed to include this subrequirement.
FAC-001-0	R2.1.5.	System protection and coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.6.	Metering and telecommunications.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.7.	Grounding and safety issues.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R2.1.8.	Insulation and insulation coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.9.	Voltage, Reactive Power, and power factor control.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.10.	Power quality impacts.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.11.	Equipment Ratings.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.12.	Synchronizing of facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.13.	Maintenance coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.14.	Operational issues (abnormal frequency and voltages).	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.15.	Inspection requirements for existing or new facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.16.	Communications and procedures during normal and emergency operating conditions.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R3.	The Transmission Owner shall maintain and update its facility connection requirements as required. The Transmission Owner shall make documentation of these requirements available to the users of the transmission system, the Regional Reliability Organization, and NERC on request (five business days).	The Transmission Owner made the requirements available more than five business days after a request, but not more than ten business days after a request.	The Transmission Owner made the requirements available more than ten business days after a request, but not more than twenty business days after a	The Transmission Owner made the requirements available more than twenty business days after a request, but not more than thirty business days after	The Transmission Owner made the requirements available more than thirty business days after a request.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				request.	a request.	
FAC-002-0	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:	The Responsible Entity failed to include in their assessment one of the subrequirements.	The Responsible Entity failed to include in their assessment two of the subrequirements.	The Responsible Entity failed to include in their assessment three of the subrequirements.	The Responsible Entity failed to include in their assessment four or more of the subrequirements.
FAC-002-0	R1.1.	Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evaluation.
FAC-002-0	R1.2.	Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity’s assessment did not include the ensurance of compliance.
FAC-002-0	R1.3.	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.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity’s assessment did not include the evidence of coordination.
FAC-002-0	R1.4.	Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance in accordance with Reliability Standard TPL-001-0.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evidence of the studies.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-002-0	R1.5.	Documentation that the assessment included study assumptions, system performance, and alternatives considered, and jointly coordinated recommendations.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the documentation.
FAC-002-0	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) Regional Reliability Organization(s) and NERC on request (within 30 calendar days).	The responsible entity provided the documentation more than 30 calendar days, but not more than 45 calendar days, after a request.	The responsible entity provided the documentation more than 45 calendar days, but not more than 60 calendar days, after a request.	The responsible entity provided the documentation more than 60 calendar days, but not more than 120 calendar days, after a request.	The responsible entity provided the documentation more than 120 calendar days after a request or was unable to provide the documentation.
FAC-003-1	R1.	The Transmission owner shall prepare, and keep current, a formal transmission vegetation management program (TVMP). The TVMP shall include the Transmission Owner's objectives, practices, approved procedures, and work Specifications. 1. ANSI A300, Tree Care Operations – Tree, Shrub, and Other Woody Plant Maintenance – Standard Practices, while not a requirement of this standard, is considered to be an industry best practice.	The applicable entity did not include and keep current one of the four required elements of its TVMP, as directed by the requirement.	The applicable entity did not include and keep current two of the four required elements of its TVMP, as directed by the requirement.	The applicable entity did not include and keep current three of the four required elements of its TVMP, as directed by the requirement.	The applicable entity did not include and keep current four of the four required elements of the TVMP, as directed by the requirement.
FAC-003-1	R1.1.	The TVMP shall define a schedule for and the type (aerial, ground) of	N/A	N/A	The applicable entity TVMP did	The applicable entity TVMP did

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ROW vegetation inspections. This schedule should be flexible enough to adjust for changing conditions. The inspection schedule shall be based on the anticipated growth of vegetation and any other environmental or operational factors that could impact the relationship of vegetation to the Transmission Owner's transmission lines.			not define a schedule, as directed by the requirement, or the type of ROW vegetation inspections, as directed by the requirement.	not define a schedule, as directed by the requirement, nor the type of ROW vegetation inspections, as directed by the requirement.
FAC-003-1	R1.2.	The Transmission Owner, in the TVMP, shall identify and document clearances between vegetation and any overhead, ungrounded supply conductors, taking into consideration transmission line voltage, the effects of ambient temperature on conductor sag under maximum design loading, and the effects of wind velocities on conductor sway. Specifically, the Transmission Owner shall establish clearances to be achieved at the time of vegetation management work identified herein as Clearance 1, and shall also establish and maintain a set of clearances identified herein as Clearance 2 to prevent flashover between vegetation and overhead ungrounded supply conductors.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not specify clearances.
FAC-003-1	R1.2.1.	Clearance 1 — The Transmission Owner shall determine and document appropriate clearance distances to be achieved at the time of transmission vegetation management work based upon local conditions and the expected time frame in which the	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not specify Clearance 1 values.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Owner plans to return for future vegetation management work. Local conditions may include, but are not limited to: operating voltage, appropriate vegetation management techniques, fire risk, reasonably anticipated tree and conductor movement, species types and growth rates, species failure characteristics, local climate and rainfall patterns, line terrain and elevation, location of the vegetation within the span, and worker approach distance requirements. Clearance 1 distances shall be greater than those defined by Clearance 2 below.				
FAC-003-1	R1.2.2.	Clearance 2 — The Transmission Owner shall determine and document specific radial clearances to be maintained between vegetation and conductors under all rated electrical operating conditions. These minimum clearance distances are necessary to prevent flashover between vegetation and conductors and will vary due to such factors as altitude and operating voltage. These Transmission Owner-specific minimum clearance distances shall be no less than those set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard 516-2003 (*Guide for Maintenance Methods on Energized Power Lines*) and as specified in its Section 4.2.2.3, Minimum Air Insulation Distances	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not specify Clearance 2 values.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		without Tools in the Air Gap.				
FAC-003-1	R1.2.2.1.	Where transmission system transient overvoltage factors are not known, clearances shall be derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.	Not Applicable.	Not Applicable.	Not Applicable.	Where transmission system transient overvoltage factors are known, clearances were not derived from Table 5, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.
FAC-003-1	R1.2.2.2.	Where transmission system transient overvoltage factors are known, clearances shall be derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.	Not Applicable.	Not Applicable.	Not Applicable.	Where transmission system transient overvoltage factors are known, clearances were not derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.
FAC-003-1	R1.3.	All personnel directly involved in the design and implementation of the TVMP shall hold appropriate qualifications and training, as defined by the Transmission Owner, to perform their duties.	One or more persons directly involved in the design and implementation of the TVMP (but not more than 35% of the all personnel involved), did not	More than 35% of all personnel directly involved in the design and implementation of the TVMP (but not more than 70% of all personnel involved), did not	More than 70% of all personnel directly involved in the design and implementation of the TVMP (but not 100% of all personnel involved), did not	None of the persons directly involved in the design and implementation of the Transmission Owner's TVMP held appropriate qualifications and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			hold appropriate qualifications and training to perform their duties.	hold appropriate qualifications and training to perform their duties.	hold appropriate qualifications and training to perform their duties.	training to perform their duties.
FAC-003-1	R1.4.	Each Transmission Owner shall develop mitigation measures to achieve sufficient clearances for the protection of the transmission facilities when it identifies locations on the ROW where the Transmission Owner is restricted from attaining the clearances specified in Requirement 1.2.1.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission Owner's TVMP does not include mitigation measures to achieve sufficient clearances where restrictions to the ROW are in effect.
FAC-003-1	R1.5.	Each Transmission Owner shall establish and document a process for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage. This is so that action (temporary reduction in line rating, switching line out of service, etc.) may be taken until the threat is relieved.	N/A	N/A	N/A	The applicable entity did not establish or did not document a process, as directed by the requirement.
FAC-003-1	R2.	The Transmission Owner shall create and implement an annual plan for vegetation management work to ensure the reliability of the system. The plan shall describe the methods used, such as manual clearing, mechanical clearing, herbicide treatment, or other actions. The plan should be flexible enough to adjust to changing conditions, taking into consideration anticipated growth of vegetation and all other	The Transmission Owner did not meet one of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of	The Transmission Owner did not meet two of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of	The Transmission Owner did not meet the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of	The Transmission Owner does not have an annual plan for vegetation management, or the Transmission Owner has not implemented the annual plan for vegetation management.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		environmental factors that may have an impact on the reliability of the transmission systems. Adjustments to the plan shall be documented as they occur. The plan should take into consideration the time required to obtain permissions or permits from landowners or regulatory authorities. Each Transmission Owner shall have systems and procedures for documenting and tracking the planned vegetation management work and ensuring that the vegetation management work was completed according to work specifications.	adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	
FAC-003-1	R3.	The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.	The Transmission Owner did not submit a quarterly report to its RRO and did not have any outages to report	The Transmission Owner did not report an outage specified as reportable in R3 to its RRO	The Transmission Owner did not report multiple outages specified as reportable in R3 to its RRO	The Transmission Owner did not report one or more outages specified as reportable in R3 to its RRO for two consecutive quarters
FAC-003-1	R3.1.	Multiple sustained outages on an individual line, if caused by the same vegetation, shall be reported as one outage regardless of the actual number of outages within a 24-hour period.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner failed to report, as a single outage, multiple sustained outages within a 24-hour period on an individual line, if caused by the same vegetation.
FAC-003-1	R3.2.	The Transmission Owner is not required to report to the RRO, or the	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner made

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		RRO's designee, certain sustained transmission line outages caused by vegetation: (1) Vegetation-related outages that result from vegetation falling into lines from outside the ROW that result from natural disasters shall not be considered reportable (examples of disasters that could create non-reportable outages include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, major storms as defined either by the Transmission Owner or an applicable regulatory body, ice storms, and floods), and (2) Vegetation-related outages due to human or animal activity shall not be considered reportable (examples of human or animal activity that could cause a non-reportable outage include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural activities or horticultural or agricultural activities, or removal or digging of vegetation).				reports for outages not considered reportable based on the categories listed in this requirement.
FAC-003-1	R3.3.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, shall include at a minimum: the name of the circuit(s) outaged, the date, time and duration of the outage; a description of the cause of the outage; other pertinent comments; and any countermeasures taken by the Transmission Owner.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include one of the required elements.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include two of the required elements.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include three of the required elements.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, did not include four or more of the required elements.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-003-1	R3.4.	An outage shall be categorized as one of the following:	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R3.4.1.	Category 1 — Grow-ins: Outages caused by vegetation growing into lines from vegetation inside and/or outside of the ROW;	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R3.4.2.	Category 2 — Fall-ins: Outages caused by vegetation falling into lines from inside the ROW;	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R3.4.3.	Category 3 — Fall-ins: Outages caused by vegetation falling into lines from outside the ROW.	Not applicable.	Not applicable.	Not applicable.	The outage was not classified in the correct category.
FAC-003-1	R4.	The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions taken by the RRO as a result of any of the reported outages.	Not applicable.	Not applicable.	The RRO did not submit a quarterly report to NERC for a single quarter.	The RRO did not submit a quarterly report to NERC for more than two consecutive quarters.
FAC-008-1	R1.	The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generation Owner does not have a documented Facility Ratings Methodology for use in developing facility ratings.
FAC-008-1	R1.1.	A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.	The Facility Rating methodology respects the most limiting applicable Equipment Rating of the individual equipment that	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate that its Facility Rating Methodology

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			comprises that Facility but there is no statement in the documentation of the methodology that states this.			respects the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
FAC-008-1	R1.2.	The method by which the Rating (of major BES equipment that comprises a Facility) is determined.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner's or Generation Owner's Facility Ratings Methodology does not specify the manner in which a rating is determined.
FAC-008-1	R1.2.1.	The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.	Not applicable.	The Transmission Owner or Generator Owner has demonstrated that it has a Facility Rating Methodology that includes methods of rating BES equipment but the equipment rating methods don't address one of the applicable required devices.	The Transmission Owner or Generator Owner has demonstrated the existence of methods of rating equipment but the equipment rating methods don't address two of the applicable required devices.	The Transmission Owner or Generator Owner has demonstrated the existence of methods of rating equipment but the equipment rating methods don't address more than two of the applicable required devices.
FAC-008-1	R1.2.2.	The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.	Not applicable.	The Transmission Owner or Generator Owner's equipment Ratings	The Transmission Owner or Generator Owner's equipment Ratings	The Transmission Owner or Generator Owner's equipment Ratings

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				methodology does address a methodology for determining emergency ratings but fails to include a methodology for determining normal ratings for its BES equipment.	methodology fails to include a methodology for determining emergency ratings for of its BES equipment.	methodology fails to demonstrate the inclusion of any method for determining normal or emergency ratings for of its BES equipment.
FAC-008-1	R1.3.	Consideration of the following:	The rating methodology did not consider one of the sub requirements.	The rating methodology did not consider two of the sub requirements.	The rating methodology did not consider three of the sub requirements.	The rating methodology did not consider four or more of the sub requirements.
FAC-008-1	R1.3.1.	Ratings provided by equipment manufacturers.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate the existence (in its Facility Rating Methodology) of how it considered ratings provided by equipment manufacturers.
FAC-008-1	R1.3.2.	Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered design criteria in developing its equipment Ratings.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-008-1	R1.3.3.	Ambient conditions.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered ambient conditions in developing its equipment Ratings.
FAC-008-1	R1.3.4.	Operating limitations.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered operating limitations in developing its equipment Ratings.
FAC-008-1	R1.3.5.	Other assumptions.	Not applicable.	Not applicable.	Not applicable.	The Transmission Owner or Generator Owner has failed to demonstrate how it considered other assumptions in developing its equipment Ratings.
FAC-008-1	R2.	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have	The Transmission Owner or Generator Owner has made its Facility Ratings Methodology available to all required entities	The Transmission Owner or Generator Owner has not made its Facility Ratings Methodology available to one of the required	The Transmission Owner or Generator Owner fails to provide its Facility Ratings Methodology available to two or more of the	The Transmission Owner or Generator Owner has not made its Facility Rating Methodology available to any of the required entities

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.	but not within 15 business days of a request.	entities, but did make the methodology available to all other required entities.	required entities.	in accordance with Requirement R2 within 60 business days of receipt of a request.
FAC-008-1	R3.	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written 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.	The responsible entity provided a response as required but took longer than 45 business days.	The responsible entity provided a response and the response indicated that a change will not be made to the Facility Ratings Methodology but did not indicate why no change will be made.	The responsible entity provided a response but the response did not indicate whether a change will be made to the Facility Ratings Methodology.	The responsible entity did not provide any evidence to demonstrate that it provided a response to a comment on its Facility Ratings Methodology in accordance with Requirement R3 within 90 business days.
FAC-009-1	R1.	The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.	The Transmission Owner or Generator Owner developed Facility Ratings for all its solely owned and jointly owned Facilities, but the ratings weren't consistent with the associated Facility Rating Methodology in	The Transmission Owner or Generator Owner developed Facility Ratings for most, but not all of its solely and jointly owned Facilities following the associated Facility Ratings Methodology	The Transmission Owner or Generator Owner developed Facility Ratings following the associated Facility Ratings Methodology but failed to develop any Facility Ratings for a significant number of its solely and	The Transmission Owner or Generator Owner has failed to demonstrate that it developed any Facility Ratings using its Facility Rating Methodology

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			one minor area.	OR the Transmission Owner or Generator Owner developed Facility Ratings for all its solely and jointly owned Facilities but failed to follow the associated Facility Ratings Methodology in one significant area.	jointly owned Facilities OR the Transmission Owner or Generator Owner has developed Facility Ratings for all its solely owned and jointly owned Facilities, but failed to follow the associated Facility Ratings Methodology in more than one significant area.	
FAC-009-1	R2.	The Transmission Owner and Generator Owner shall each 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 Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to 15 calendar days.	The Transmission Owner or Generator Owner provided its Facility Ratings to all but one of the requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to two of the requesting entities.	The Transmission Owner or Generator Owner has provided its Facility Ratings to none of the requesting entities within 30 calendar days of the associated schedules.
FAC-010-2	R1	The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL	Not applicable.	The Planning Authority has a documented SOL Methodology for	The Planning Authority has a documented SOL Methodology for	The Planning Authority has a documented SOL Methodology for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Methodology shall:		use in developing SOLs within its Planning Authority Area, but it does not address R1.2	use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	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.
FAC-010-2	R1.1.	Be applicable for developing SOLs used in the planning horizon.	Not applicable.	Not applicable.	Not applicable.	Planning Authority SOL methodology is not applicable for developing SOL in the planning horizon.
FAC-010-2	R1.2.	State that SOLs shall not exceed associated Facility Ratings.	Not applicable.	Not applicable.	Not applicable.	Planning Authority SOL Methodology did not state that SOLs shall not exceed associated Facility Ratings
FAC-010-2	R1.3.	Include a description of how to identify the subset of SOLs that qualify as IROLs.	Not applicable.	Not applicable.	Not applicable.	Planning Authority SOL Methodology did not include a description of how to identify the subset of SOLs that qualify as IROLs.
FAC-010-2	R2.	The Planning Authority's SOL				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Methodology shall include a requirement that SOLs provide BES performance consistent with the following				
FAC-010-2	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.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority's methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.1.
FAC-010-2	R2.2.	Following the single Contingencies 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.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority's methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.2.
FAC-010-2	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.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						transformer, or shunt device.
FAC-010-2	R2.2.2.	Loss of any generator, line, transformer, or shunt device without a Fault.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address the loss of any generator, line, transformer, or shunt device without a Fault.
FAC-010-2	R2.2.3.	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
FAC-010-2	R2.3.	Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:	Not applicable.	Not applicable.	Not applicable.	The methodology does not include one or more of the following: 2.3.1. through 2.3.3.
FAC-010-2	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.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that starting with all Facilities in service, the system's response to a single Contingency may include planned or controlled

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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.
FAC-010-2	R2.3.2.	System reconfiguration through manual or automatic control or protection actions.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that starting with all Facilities in service, the system's response to a single Contingency may include System reconfiguration through manual or automatic control or protection actions.
FAC-010-2	R2.4.	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that in order to prepare for the next Contingency, system adjustments may be made, including changes to generation, uses

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						of the transmission system, and the transmission system topology.
FAC-010-2	R2.5.	Starting with all Facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 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.	Not applicable.	Not applicable.	Not applicable.	The SOL methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.5.
FAC-010-2	R2.6.	In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:	Not applicable.	Not applicable.	Not applicable.	Not applicable.
FAC-010-2	R2.6.1.	Planned or 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.	Not applicable.	Not applicable.	Not applicable.	The SOL Methodology does not provide that in determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Planned or 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 shall be acceptable.
FAC-010-2	R3.	The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	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.
FAC-010-2	R3.1.	Study model (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a study model that includes the entire Planning Authority Area, and the critical modeling details of other Planning Authority Areas that would

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						impact the facility or facilities under study.
FAC-010-2	R3.2.	Selection of applicable Contingencies.	Not applicable.	Not applicable.	Not applicable.	The methodology does not include the selection of applicable Contingencies.
FAC-010-2	R3.3	Level of detail of system models used to determine SOLs.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the level of detail of system models used to determine SOLs.
FAC-010-2	R3.4.	Allowed uses of Special Protection Systems or Remedial Action Plans.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the allowed uses of Special Protection Systems or Remedial Action Plans.
FAC-010-2	R3.5.	Anticipated transmission system configuration, generation dispatch and Load level.	Not applicable.	Not applicable.	Not applicable.	The methodology does not include the description of anticipated transmission system configuration, generation dispatch and Load level.
FAC-010-2	R3.6.	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a description of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Limit (IROL) and criteria for developing any associated IROL T_v.				criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.
FAC-010-2	R4.	The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:	One or both of the following: The Planning Authority 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 provided up to 30 calendar days after the effectiveness of the change.	One of the following: 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 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR	One of the following: 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 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its	One of the following: The Planning Authority failed to issue its SOL Methodology and 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				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.	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.	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,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						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 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.
FAC-010-2	R4.1.	Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not issue its SOL Methodology and any change to that methodology, prior to the effectiveness of the change, to each adjacent Planning Authority and each Planning

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Authority that indicated it has a reliability-related need for the methodology.
FAC-010-2	R4.2.	Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not issue its SOL Methodology and any change to that methodology, prior to the effectiveness of the change, to each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.
FAC-010-2	R4.3.	Each Transmission Planner that works in the Planning Authority's Planning Authority Area.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not issue its SOL Methodology and any change to that methodology, prior to the effectiveness of the change, to each Transmission Planner that works in the Planning Authority's

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Planning Authority Area prior to the effectiveness of the change.
FAC-010-2	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority 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 SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	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.	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.	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. OR 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.	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. OR 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.
FAC-011-2	R1.	The Reliability Coordinator shall have a documented methodology for	Not applicable.	The Reliability Coordinator has a	The Reliability Coordinator has a	The Reliability Coordinator has a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:		documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	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.
FAC-011-2	R1.1.	Be applicable for developing SOLs used in the operations horizon.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator's SOL methodology is not applicable for developing SOL in the operations horizon.
FAC-011-2	R1.2.	State that SOLs shall not exceed associated Facility Ratings.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator's SOL Methodology did not state that SOLs shall not exceed associated Facility Ratings
FAC-011-2	R1.3	Include a description of how to identify the subset of SOLs that	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator's SOL

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		qualify as IROLs				Methodology did not include a description of how to identify the subset of SOLs that qualify as IROLs.
FAC-011-2	R2.	The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:				
FAC-011-2	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.	Not applicable.	Not applicable.	Not applicable.	The SOL methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.1.
FAC-011-2	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.	Not applicable.	Not applicable.	Not applicable.	The SOL methodology does not include a requirement that SOLs provide BES performance consistent with sub-requirement R2.2.
FAC-011-2	R2.2.1.	Single line to ground or 3-phase Fault (whichever is more severe), with	Not applicable.	Not applicable.	Not applicable.	The methodology does not require

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Normal Clearing, on any Faulted generator, line, transformer, or shunt device				that SOLs provide BES performance consistent with: single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
FAC-011-2	R2.2.2.	Loss of any generator, line, transformer, or shunt device without a Fault.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address the loss of any generator, line, transformer, or shunt device without a Fault.
FAC-011-2	R2.2.3.	Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
FAC-011-2	R2.3.	In determining the system's response to a single Contingency, the following shall be acceptable:	Not applicable.	Not applicable.	Not applicable.	The methodology does not include one or more of the following 2.3.1. through 2.3.3.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-011-2	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.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address that, in determining the systems response to a single contingency, 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 is acceptable.
FAC-011-2	R2.3.2.	Interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies	Not applicable.	Not applicable.	Not applicable.	The methodology does not address that, in determining the systems response to a single contingency, Interruption of other network customers is acceptable, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						operating conditions are more adverse than anticipated in the corresponding studies.
FAC-011-2	R2.3.3.	System reconfiguration through manual or automatic control or protection actions.	Not applicable.	Not applicable.	Not applicable.	The methodology does not address that, in determining the systems response to a single contingency, system reconfiguration through manual or automatic control or protection actions is acceptable.
FAC-011-2	R2.4.	To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.	Not applicable.	Not applicable.	Not applicable.	The methodology does not provide that to prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.
FAC-011-2	R3.	The Reliability Coordinator's methodology for determining SOLs,	The Reliability Coordinator has a	The Reliability Coordinator has a	The Reliability Coordinator has a	The Reliability Coordinator has a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.7.
FAC-011-2	R3.1.	Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a description of the study model to be used which must include the entire Reliability Coordinator area, and the critical details of other Reliability Coordinator areas that would impact the facility or facilities under study
FAC-011-2	R3.2.	Selection of applicable Contingencies	Not applicable.	Not applicable.	Not applicable.	The methodology does not include the selection of applicable Contingencies.
FAC-011-2	R3.3.	A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use	Not applicable.	Not applicable.	Not applicable.	The methodology does not include a description of a process for determining which of the stability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		in the operating horizon given the actual or expected system conditions.				limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.
FAC-011-2	R3.3.1.	This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies	Not applicable.	Not applicable.	Not applicable.	The methodology for determining SOL's does not address the need to modify the limits described in R3.3, the list of limits, or the list of associated multiple contingencies.
FAC-011-2	R3.4.	Level of detail of system models used to determine SOLs.	Not applicable.	Not applicable.	Not applicable.	Methodology does not describe the level of detail of system models used to determine SOLs.
FAC-011-2	R3.5.	Allowed uses of Special Protection Systems or Remedial Action Plans.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the allowed uses of Special Protection

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems or Remedial Action Plans.
FAC-011-2	R3.6.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe the anticipated transmission system configuration, generation dispatch and Load level.	
FAC-011-2	R3.7.	Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.	Not applicable.	Not applicable.	Not applicable.	The methodology does not describe criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit and criteria for developing any associated IROL T_v.
FAC-011-2	R4	The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:	One or both of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the	One of the two following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities	One of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	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 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.	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 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	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 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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					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.	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,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the changed methodology was provided up to 30 calendar days after the effectiveness of the change
FAC-011-2	R4.1.	Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not issue its SOL Methodology or any changes to that methodology to each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.
FAC-011-2	R4.2.	Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not issue its SOL Methodology or any changes to that methodology to each Planning Authority or Transmission Planner that models any portion of the Reliability Coordinator's Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Coordinator Area.
FAC-011-2	R4.3.	Each Transmission Operator that operates in the Reliability Coordinator Area.	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not issue its SOL Methodology or any changes to that methodology to each Transmission Operator that operates in the Reliability Coordinator Area.
FAC-011-2	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability 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 SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	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.	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.	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	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

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					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.	comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.
FAC-013-1	R1.	The Reliability Coordinator and Planning Authority shall each establish a set of inter-regional and intra-regional Transfer Capabilities that is consistent with its current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but one or more Transfer Capabilities, but not more than 25% of all Transfer Capabilities required to be established, are not consistent with the current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but more than 25% of those Transfer Capabilities, but not more than 50% of all Transfer Capabilities required to be established, are not consistent with the current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but more than 50% of those Transfer Capabilities, but not more than 75% of all Transfer Capabilities required to be established, are not consistent with the current Transfer Capability Methodology.	The Reliability Coordinator or Planning Authority has established a set of Transfer Capabilities, but more than 75% of those Transfer Capabilities are not consistent with the current Transfer Capability Methodology OR The Reliability Coordinator or Planning Authority has not established a set of Transfer Capabilities.
FAC-013-1	R2.	The Reliability Coordinator and Planning Authority shall each provide its inter-regional and intra-regional	The Reliability Coordinator or Planning Authority	The Reliability Coordinator or Planning Authority	The Reliability Coordinator or Planning Authority	The Reliability Coordinator or Planning Authority

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transfer Capabilities to those entities that have a reliability-related need for such Transfer Capabilities and make a written request that includes a schedule for delivery of such Transfer Capabilities as follows:	has provided its Transfer Capabilities but missed meeting one schedule by up to 15 calendar days.	has provided its Transfer Capabilities but missed meeting two schedules.	has provided its Transfer Capabilities but missed meeting more than two schedules.	has provided its Transfer Capabilities but missed meeting all schedules within 30 calendar days of the associated schedules.
FAC-013-1	R2.1.	The Reliability Coordinator shall provide its Transfer Capabilities to its associated Regional Reliability Organization(s), to its adjacent Reliability Coordinators, and to the Transmission Operators, Transmission Service Providers and Planning Authorities that work in its Reliability Coordinator Area.	Not applicable.	The Reliability Coordinator provided its Transfer Capabilities to all but one of the required entities.	The Reliability Coordinator failed to provide its Transfer Capabilities to more than one of the required entities.	The Reliability Coordinator provided its Transfer Capabilities to none of the required entities.
FAC-013-1	R2.2.	The Planning Authority shall provide its Transfer Capabilities to its associated Reliability Coordinator(s) and Regional Reliability Organization(s), and to the Transmission Planners and Transmission Service Provider(s) that work in its Planning Authority Area.	Not applicable.	The Planning Authority provided its Transfer Capabilities to all but one of the required entities.	The Planning Authority failed to provide its Transfer Capabilities to more than one of the required entities.	The Planning Authority provided its Transfer Capabilities to none of the required entities.
FAC-014-2	R1.	The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.	There are SOLs, for the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs for the Reliability Coordinator Area, but one or more of these the SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-014-2	R2.	The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 75% or more of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)
FAC-014-2	R3.	The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology	There are SOLs, for the Planning Coordinator Area, but from 1% up to, but less than, 25% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs, for the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are Sols for the Planning Coordinator Area, but 10% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	There are SOLs, for the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)
FAC-014-2	R4.	The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology.	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but up to 25% of these SOLs are inconsistent with the Planning Coordinator's SOL	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL	The Transmission Planner has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but one or more of these SOLs are inconsistent with the Planning Coordinator's SOL

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Methodology. (R4)	Methodology. (R4)	Methodology. (R4)	Methodology. (R4)
FAC-014-2	R5.	The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows	The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules by less than 15 calendar days. (R5)	One of the following: The responsible entity provided its SOLs to all but one of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 15 or more but less than 30 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.4	One of the following: The responsible entity provided its SOLs to all but two of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 30 or more but less than 45 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.3	One of the following: The responsible entity failed to provide its SOLs to more than two of the requesting entities within 45 calendar days of the associated schedules. (R5) OR The supporting information provided with the IROLs does not address 5.1.1 and 5.1.2.
FAC-014-2	R5.1.	The Reliability Coordinator shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Reliability Coordinators and Reliability Coordinators who indicate	Not applicable.	Not applicable.	Not applicable.	The Reliability Coordinator did not provide its SOLs (including the subset of SOLs that

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area. For each IROL, the Reliability Coordinator shall provide the following supporting information				are IROLs) to adjacent Reliability Coordinators and Reliability Coordinators who indicate a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area.
FAC-014-2	R5.1.1.	Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL.
FAC-014-2	R5.1.2.	The value of the IROL and its associated Tv.	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the value

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						of the IROL and its associated Tv.
FAC-014-2	R5.1.3.	The associated Contingency (ies).	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the associated Contingency(ies).
FAC-014-2	R5.1.4.	The type of limitation represented by the IROL (e.g., voltage collapse, angular stability).	Not applicable.	Not applicable.	Not applicable.	For any IROL, the Reliability Coordinator did not provide the type of limitation represented by the IROL (e.g., voltage collapse, angular stability).
FAC-014-2	R5.2.	The Transmission Operator shall provide any SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.	Not applicable.	Not applicable.	Not applicable.	The Transmission Operator did not provide the complete set of SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.
FAC-014-2	R5.3.	The Planning Authority shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Planning Authorities, and to	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not provide its complete set of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Planners, Transmission Service Providers, Transmission Operators and Reliability Coordinators that work within its Planning Authority Area.				SOLs (including the subset of SOLs that are IROLs) to adjacent Planning Authorities, and to Transmission Planners, Transmission Service Providers, Transmission Operators and Reliability Coordinators that work within its Planning Authority Area.
FAC-014-2	R5.4.	The Transmission Planner shall provide its SOLs (including the subset of SOLs that are IROLs) to its Planning Authority, Reliability Coordinators, Transmission Operators, and Transmission Service Providers that work within its Transmission Planning Area and to adjacent Transmission Planners.	Not applicable.	Not applicable.	Not applicable.	The Transmission Planner did not provide its complete set of SOLs (including the subset of SOLs that are IROLs) to its Planning Authority, Reliability Coordinators, Transmission Operators, and Transmission Service Providers that work within its Transmission Planning Area and to adjacent

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Transmission Planners.
FAC-014-2	R6.	The Planning Authority shall identify the subset of multiple contingencies (if any), from Reliability Standard TPL-003 which result in stability limits.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not identify the subset of multiple contingencies which result in stability limits. (R6)
FAC-014-2	R6.1.	The Planning Authority shall provide this list of multiple contingencies and the associated stability limits to the Reliability Coordinators that monitor the facilities associated with these contingencies and limits.	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not identify the subset of multiple contingencies, from TPL-003 that resulted in stability limits and provide the complete list of multiple contingencies and the associated stability limits to the Reliability Coordinators that monitor the facilities associated with these contingencies and limits.
FAC-014-2	R6.2.	If the Planning Authority does not identify any stability-related multiple contingencies, the Planning Authority	Not applicable.	Not applicable.	Not applicable.	The Planning Authority did not notify the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall so notify the Reliability Coordinator.				Reliability Coordinator that it did not identify any stability-related multiple contingencies,

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-001-3	R1.	The Load-Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for:	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)
INT-001-3	R1.1.	All Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.
INT-001-3	R2.	The Sink Balancing Authority shall ensure that Arranged Interchange is submitted to the Interchange Authority:	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)
INT-001-3	R2.1.	If a Purchasing-Selling Entity is not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.
INT-001-3	R2.2.	For each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.
INT-003-2	R1.	Each Receiving Balancing Authority shall confirm Interchange Schedules with the Sending Balancing Authority prior to implementation in the Balancing Authority's ACE equation.	There shall be a separate Lower VSL, if either of the following conditions exists: One instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. One instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	There shall be a separate Moderate VSL, if either of the following conditions exists: Two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Two instances of not coordinating the Interchange	There shall be a separate High VSL, if either of the following conditions exists: Three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Three instances of not coordinating the Interchange	There shall be a separate Severe VSL, if either of the following conditions exists: Four or more instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Four or more instances of not coordinating the Interchange

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-003-2	R1.1.	The Sending Balancing Authority and Receiving Balancing Authority shall agree on Interchange as received from the Interchange Authority, including:	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-2	R1.1.1.	Interchange Schedule start and end time.	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-2	R1.1.2.	Energy profile.	The Balancing Authority experienced one instance of entering a schedule into its ACE equation	The Balancing Authority experienced two instances of entering a schedule into its ACE equation	The Balancing Authority experienced three instances of entering a schedule into its ACE equation	The Balancing Authority experienced four instances of entering a schedule into its ACE equation

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-2	R1.2.	If a high voltage direct current (HVDC) tie is on the Scheduling Path, then the Sending Balancing Authorities and Receiving Balancing Authorities shall coordinate the Interchange Schedule with the Transmission Operator of the HVDC tie.	The sending or receiving Balancing Authority experienced one instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced two instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced three instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced four instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-004-2	R1.	At such time as the reliability event allows for the reloading of the transaction, the entity that initiated the curtailment shall release the limit on the Interchange Transaction tag to allow reloading the transaction and shall communicate the release of the limit to the Sink Balancing Authority.	The entity that initiated the curtailment failed to communicate the transaction reload to the Sink Balancing Authority	The entity that initiated the curtailment failed to reload the transaction and failed to communicate to the Sink Balancing Authority	N/A	N/A
INT-004-2	R2.	The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:	The Purchase-Selling entity failed to update the tags when required less than 25% of times it was required, as determined in R2.1, R2.2, or R2.3.	The Purchase-Selling entity failed to update the tags when required 25% or more and less than 50% of the times it was required, as determined in R2.1, R2.2, or R2.3.	The Purchase-Selling entity failed to update the tags when required 50% or more but less than75% of the times it was required, as determined in R2.1, R2.2, or R2.3.	The Purchase-Selling entity failed to update the tags when required 75% or more of the times it was required, as determined in R2.1, R2.2, or R2.3.
INT-004-2	R2.1.	The average energy profile in an hour is greater than 250 MW	The Purchase-Selling entity failed to update	The Purchase-Selling entity failed to update	The Purchase-Selling entity failed to update	The Purchase-Selling entity failed to update

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +10%.	the tags when required less than 25% of times it was required.	the tags when required 25% or more and less than 50% of the times it was required.	the tags when required 50% or more but less than75% of the times it was required.	the tags when required 75% or more of the times it was required.
INT-004-2	R2.2.	The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +25 megawatt-hours.	The Purchase-Selling entity failed to update the tags when required less than 25% of times it was required.	The Purchase-Selling entity failed to update the tags when required 25% or more and less than 50% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 50% or more but less than75% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 75% or more of the times it was required.
INT-004-2	R2.3.	A Reliability Coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons.	The Purchase-Selling entity failed to update the tags when required less than 25% of times it was required.	The Purchase-Selling entity failed to update the tags when required 25% or more and less than 50% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 50% or more but less than75% of the times it was required.	The Purchase-Selling entity failed to update the tags when required 75% or more of the times it was required.
INT-005-2	R1.	Prior to the expiration of the time period defined in the Timing Table, Column A, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment to all reliability entities involved in the Interchange.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities
INT-005-2	R1.1.	When a Balancing Authority or Reliability Coordinator initiates a Curtailment to Confirmed or Implemented Interchange for reliability, the Interchange	The Interchange Authority experienced one occurrence of not distributing information to all	The Interchange Authority experienced two occurrences of not distributing information to all	The Interchange Authority experienced three occurrences of not distributing information to all	The Interchange Authority experienced four occurrences of not distributing information to all

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authority shall distribute the Arranged Interchange information for reliability assessment only to the Source Balancing Authority and the Sink Balancing Authority.	involved reliability entities.	involved reliability entities	involved reliability entities	involved reliability entities
INT-006-2	R1.	Prior to the expiration of the reliability assessment period defined in the Timing Table, Column B, the Balancing Authority and Transmission Service Provider shall respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on one occasion to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on two occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on three occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	The Responsible Entity failed on four occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.
INT-006-2	R1.1.	Each involved Balancing Authority shall evaluate the Arranged Interchange with respect to:	The Balancing Authority failed to evaluate arranged interchange with respect to one of the requirements in the 3 sub-components.	N/A	The Balancing Authority failed to evaluate arranged interchange with respect to two of the requirements in the 3 sub-components.	The Balancing Authority failed to evaluate arranged interchange with respect to three of the requirements in the 3 sub-components.
INT-006-2	R1.1.1.	Energy profile (ability to support the magnitude of the Interchange).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Energy profile (ability to support the magnitude of the Interchange).
INT-006-2	R1.1.2.	Ramp (ability of generation maneuverability to accommodate).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Ramp (ability of generation maneuverability to accommodate).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-006-2	R1.1.3.	Scheduling path (proper connectivity of Adjacent Balancing Authorities).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Scheduling path (proper connectivity of Adjacent Balancing Authorities).
INT-006-2	R1.2.	Each involved Transmission Service Provider shall confirm that the transmission service arrangements associated with the Arranged Interchange have adjacent Transmission Service Provider connectivity, are valid and prevailing transmission system limits will not be violated.	The Transmission Service Provider experienced one instance of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced two instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced three instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experience four instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.
INT-007-1	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:	The Interchange Authority failed to verify one time, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed	The Interchange Authority failed to verify two times, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed	The Interchange Authority failed to verify three times, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed	The Interchange Authority failed to verify four times, as indicated in R1.1, R1.2, R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interchange.	Interchange.	Interchange.	Interchange.
INT-007-1	R1.1.	Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.2.	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.	The following are defined:	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.1.	Generation source and load sink.	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.2.	Megawatt profile.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.3.	Ramp start and stop times.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.4.	Interchange duration.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	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.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with minor exception and is substantially compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with some exception and is mostly compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval but was substantially deficient in meeting the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment did not provided approval and failed to meet the requirement.
INT-008-2	R1.	Prior to the expiration of the time period defined in the Timing Table, Column C, the Interchange Authority shall distribute to all Balancing Authorities (including Balancing Authorities on both sides of a direct current tie), Transmission Service Providers and Purchasing-Selling Entities involved in the Arranged Interchange whether or not the Arranged Interchange has transitioned to a Confirmed	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as deliniated in R1.1, R1.1.1 or R1.1.2.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities or no evidence provided.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Interchange.				
INT-008-2	R1.1.	For Confirmed Interchange, the Interchange Authority shall also communicate:	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-2	R1.1.1.	Start and stop times, ramps, and megawatt profile to Balancing Authorities.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-2	R1.1.2.	Necessary Interchange information to NERC-identified reliability analysis services.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-009-1	R1.	The Balancing Authority shall implement Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced one occurrence of not implementing a Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced two occurrences of not implementing a Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced three occurrences of not implementing a Confirmed Interchange as received from the Interchange Authority.	The Balancing Authority experienced four occurrences of not implementing a Confirmed Interchange as received from the Interchange Authority.

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-010-1	R1.	The Balancing Authority that experiences a loss of resources covered by an energy sharing agreement shall ensure that a request for an Arranged Interchange is submitted with a start time no more than 60 minutes beyond the resource loss. If the use of the energy sharing agreement does not exceed 60 minutes from the time of the resource loss, no request for Arranged Interchange is required.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed one time to submit a request for an Arranged Interchange within the specified time period.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed two times to submit request for an Arranged Interchange within the specified time period.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed three times to submit a request for an Arranged Interchange within the specified time period.	The Balancing Authority that experienced a loss of resource covered by an energy sharing agreement failed four or more times to submit a request for an Arranged Interchange within the specified time period.
INT-010-1	R2.	For a modification to an existing Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit the modified Arranged Interchange reflecting that modification within 60 minutes of the initiation of the event.	The Reliability Coordinator failed one time to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed one time to submit the modified schedule as directed.	The Reliability Coordinator failed two times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed two times to submit the modified schedule as directed.	The Reliability Coordinator failed three times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed three times to submit the modified schedule as directed.	The Reliability Coordinator failed four times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed four times to submit the modified schedule as directed.
INT-010-1	R3.	For a new Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit an Arranged Interchange reflecting that Interchange schedule within 60 minutes of	The Reliability Coordinator failed one time to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed one time to submit a schedule as directed.	The Reliability Coordinator failed two times to direct the submittal of a new or modified Arranged Interchange ; or the Balancing Authority failed two times to submit a schedule as directed.	The Reliability Coordinator failed three times to direct the submittal of a new or modified Arranged Interchange ; or the Balancing Authority failed three times to submit a schedule as directed.	The Reliability Coordinator failed four times to direct the submittal of a new or modified Arranged Interchange; or the Balancing Authority failed four times or more to submit a schedule as directed.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the initiation of the event.				

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-001-1.1	R1.	Each Regional Reliability Organization, subregion, or interregional coordinating group shall establish one or more Reliability Coordinators to continuously assess transmission reliability and coordinate emergency operations among the operating entities within the region and across the regional boundaries.	The RRO, subregion or interregional coordinating group did not communicate the assignment of the Reliability Coordinators to operating entities clearly.	The RRO, subregion or interregional coordinating group did not clearly identify the coordination of Reliability Coordinator areas within the region.	The RRO, subregion or interregional coordinating group did not coordinate assignment of the Reliability Coordinators across regional boundaries.	The RRO, subregion or interregional coordinating group did not assign any Reliability Coordinators.
IRO-001-1.1	R2.	The Reliability Coordinator shall comply with a regional reliability plan approved by the NERC Operating Committee.	The Reliability Coordinator has failed to follow the administrative portions of its regional reliability plan.	The Reliability Coordinator has failed to follow steps in its regional reliability plan that requires operator interventions or actions.	The Reliability Coordinator does not have a regional reliability plan approved by the NERC OC.	The Reliability Coordinator does not have an unapproved regional reliability plan.
IRO-001-1.1	R3.	The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes.	N/A	N/A	The Reliability Coordinator cannot demonstrate that it has clear authority to act or direct actions to preserve transmission security and reliability of the Bulk Electric System.	The Reliability Coordinator failed to take or direct to preserve the reliability and security of the Bulk Electric System within 30 minutes of identifying those actions.
IRO-001-1.1	R4.	Reliability Coordinators that delegate tasks to other entities shall have formal	1. Less than 25% of the tasks are not	1. More than 25% but 50% or less of	1. More than 50% but 75% or less of	1. There is no formal operating agreement

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		operating agreements with each entity to which tasks are delegated. The Reliability Coordinator shall verify that all delegated tasks are understood, communicated, and addressed within its Reliability Coordinator Area. All responsibilities for complying with NERC and regional standards applicable to Reliability Coordinators shall remain with the Reliability Coordinator.	documented in the agreement or 2. Less than 25% of the tasks are not performed according to the agreement.	the tasks are not documented in the agreement or 2. More than 25% but 50% or less of the tasks are not performed according to the agreement.	the tasks are not documented in the agreement or 2. More than 50% but 75% or less of the tasks are not performed according to the agreement.	for tasks delegated by the Reliability Coordinator, 2. More than 75% of the tasks are not documented in the agreement or 3. More than 75% of the tasks are not performed according to the agreement.
IRO-001-1.1	R5.	The Reliability Coordinator shall list within its reliability plan all entities to which the Reliability Coordinator has delegated required tasks.	25% or less of the delegate entities are not identified in the reliability plan.	More than 25% but 50% or less of the delegate entities are not identified in the reliability plan.	More than 50% but 75% or less of the delegate entities are not identified in the reliability plan.	1. There is no reliability plan or 2. More than 75% of the delegate entities are not identified in the reliability plan.
IRO-001-1.1	R6.	The Reliability Coordinator shall verify that all delegated tasks are carried out by NERC-certified Reliability Coordinator operating personnel.	N/A	1. The Reliability Coordinator has failed to demonstrate at least one delegated task was performed by NERC certified Reliability Coordinator operating personnel or 2. The Reliability Coordinator did not require the delegate entity to have NERC certified Reliability Coordinator operating	1. The Reliability Coordinator has failed to demonstrate at least one delegated task was performed by NERC certified Reliability Coordinator operating personnel and did not require the delegate entity to have NERC certified Reliability Coordinator operating personnel or 2. The Reliability Coordinator has	The Reliability Coordinator has failed to demonstrate any delegated tasks were performed by NERC certified Reliability Coordinator operating personnel and did not require the delegate entity to have NERC certified Reliability Coordinator operating personnel.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				personnel.	failed to demonstrate at least two delegated task were performed by NERC certified Reliability Coordinator operating personnel.	
IRO-001-1.1	R7.	The Reliability Coordinator shall have clear, comprehensive coordination agreements with adjacent Reliability Coordinators to ensure that System Operating Limit or Interconnection Reliability Operating Limit violation mitigation requiring actions in adjacent Reliability Coordinator Areas are coordinated.	The Reliability Coordinator has demonstrated the existence of coordination agreements with adjacent Reliability Coordinators but the agreements are not clear or comprehensive.	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to mitigate SOL or IROL violations in its own Reliability Coordinator area.	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to mitigate SOL and IROL violations in its own Reliability Coordinator area.	The Reliability Coordinator has failed to demonstrate the existence of any coordination agreements with adjacent Reliability Coordinators.
IRO-001-1.1	R8.	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities did not follow

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.	Entities, and Purchasing-Selling Entities followed the Reliability Coordinators directive with a delay not caused by equipment problems but did notify the Reliability Coordinator of the delay.	Entities, and Purchasing-Selling Entities followed the Reliability Coordinators directive with a delay not caused by equipment problems and did not notify the Reliability Coordinator of the delay.	Entities, and Purchasing-Selling Entities followed the majority of the Reliability Coordinators directive and did not notify the Reliability Coordinator that it could not fully follow the directive because it would violate safety, equipment, statutory or regulatory requirements.	the Reliability Coordinators directive and did not notify the Reliability Coordinator that it could not follow the directive because it would violate safety, equipment, statutory or regulatory requirements.
IRO-001-1.1	R9.	The Reliability Coordinator shall act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of any other entity.	N/A	N/A	N/A	The Reliability Coordinator did not act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of one or more other entities.
IRO-002-1	R1.	Each Reliability Coordinator shall have adequate communications facilities (voice and data links) to appropriate entities within its Reliability Coordinator Area. These communications facilities shall be staffed and available to act in addressing a real-time emergency	The Reliability Coordinator has demonstrated communication facilities for both voice and data exist to all appropriate entities and that	The Reliability Coordinator has failed to demonstrate that is has: 1) Voice communication links with one	The Reliability Coordinator has failed to demonstrate that is has: 1) Voice communication links with two	The Reliability Coordinator has failed to demonstrate that is has: 1) Voice communication links with more than two appropriate entities or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		condition.	they are staffed and available but they are less than adequate.	appropriate entity or 2) Data links with one appropriate entity.	appropriate entities or 2) Data links with two appropriate entities.	2) Data links with more than two appropriate entities or 3) Communication facilities are not staffed or 4) Communication facilities are not ready.
IRO-002-1	R2.	Each Reliability Coordinator shall determine the data requirements to support its reliability coordination tasks and shall request such data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities, or adjacent Reliability Coordinators.	The Reliability Coordinator demonstrated that it 1) determined its data requirements and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators with a material impact on the Bulk Electric System in its Reliability Coordination Area but did not request	The Reliability Coordinator demonstrated that it determined the majority but not all of its data requirements necessary to support its reliability coordination functions and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability	The Reliability Coordinator demonstrated that it determined 1) some but less than the majority of its data requirements necessary to support its reliability coordination functions and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent	The Reliability Coordinator failed to demonstrate that it 1) determined its data requirements necessary to support its reliability coordination functions and requested that data from its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators or 2) requested the data from three or more of its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the data from Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators with minimal impact on the Bulk Electric System in its Reliability Coordination Area or 2) determined its data requirements necessary to perform its reliability functions with the exceptions of data that may be needed for administrative purposes such as data reporting.	Coordinators.	Reliability Coordinators or 2) all of its data requirements necessary to support its reliability coordination functions but failed to demonstrate that it requested data from two of its Transmission Operators, Balancing Authorities, Transmission Owners, Generation Owners, Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators.	Generation Operators, and Load-Serving Entities or Adjacent Reliability Coordinators.
IRO-002-1	R3.	Each Reliability Coordinator – or its Transmission Operators and Balancing Authorities – shall provide, or arrange provisions for, data exchange to other	N/A	The Reliability Coordinator or designated Transmission	The Reliability Coordinator or designated Transmission	The Reliability Coordinator or designated Transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinators or Transmission Operators and Balancing Authorities via a secure network.		Operator and Balancing Authority has failed to demonstrate it provided or arranged provision for the exchange of data with one of the other Reliability Coordinators or Transmission Operators and Balancing Authorities.	Operator and Balancing Authority has failed to demonstrate it provided or arranged provision for the exchange of data with two of the other Reliability Coordinators or Transmission Operators and Balancing Authorities.	Operator and Balancing Authority has failed to demonstrate it provided or arranged provision for the exchange of data with three of the other Reliability Coordinators or Transmission Operators and Balancing Authorities.
IRO-002-1	R4.	Each Reliability Coordinator shall have multi-directional communications capabilities with its Transmission Operators and Balancing Authorities, and with neighboring Reliability Coordinators, for both voice and data exchange as required to meet reliability needs of the Interconnection.	N/A	The Reliability Coordinator has failed to demonstrate multi-directional communication capabilities to one of the Transmission Operators and Balancing Authorities in its Reliability Coordinator Area and with neighboring Reliability Coordinators.	The Reliability Coordinator has failed to demonstrate multi-directional communication capabilities to two or more of the Transmission Operators and Balancing Authorities in its Reliability Coordinator Area and with neighboring Reliability Coordinators.	The Reliability Coordinator has failed to demonstrate multi-directional communication capabilities to all of the Transmission Operators and Balancing Authorities in its Reliability Coordinator Area and with all neighboring Reliability Coordinators.
IRO-002-1	R5.	Each Reliability Coordinator shall have detailed real-time monitoring capability of its Reliability Coordinator Area and sufficient monitoring capability of its	The Reliability Coordinator's monitoring systems provide	The Reliability Coordinator has failed to demonstrate that is	The Reliability Coordinator has failed to demonstrate that is	The Reliability Coordinator has failed to demonstrate that is has detailed real-time

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		surrounding Reliability Coordinator Areas to ensure that potential or actual System Operating Limit or Interconnection Reliability Operating Limit violations are identified. Each Reliability Coordinator shall have monitoring systems that provide information that can be easily understood and interpreted by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant and highly reliable infrastructure.	information in a way that is not easily understood and interpreted by the Reliability Coordinator's operating personnel or particular emphasis was not given to alarm management and awareness systems, automated data transfers and synchronized information systems.	has detailed real-time monitoring capabilities in its Reliability Coordinator Area and sufficient monitoring capabilities of its surrounding Reliability Coordinator Areas to ensure that one potential or actual SOL or IROL violation is not identified.	has detailed real-time monitoring capabilities in its Reliability Coordinator Area and sufficient monitoring capabilities of its surrounding Reliability Coordinator Areas to ensure that two or more potential and actual SOL and IROL violations are not identified.	monitoring capabilities in its Reliability Coordinator Area and sufficient monitoring capabilities of its surrounding Reliability Coordinator Areas to ensure that all potential and actual SOL and IROL violations are identified.
IRO-002-1	R6.	Each Reliability Coordinator shall monitor Bulk Electric System elements (generators, transmission lines, buses, transformers, breakers, etc.) that could result in SOL or IROL violations within its Reliability Coordinator Area. Each Reliability Coordinator shall monitor both real and reactive power system flows, and operating reserves, and the status of Bulk Electric System elements that are or could be critical to SOLs and IROLs and system restoration requirements within its Reliability Coordinator Area.	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements that could result in one SOL violations or 2) or operating reserves for a small portion of the Reliability Authority Area.	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing one IROL or to system restoration, 2) the status, real power flow or reactive power flow of Bulk Electric System elements that could result in multiple SOL violations, or	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing two or more IROLs; or one IROL and to system restoration, 2) the status, real power flow or reactive power flow of Bulk Electric System elements that could result in	The Reliability Coordinator failed to monitor: 1) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing all IROLs and to system restoration, or 2) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing all SOL violations and operating reserves.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) operating reserves.	multiple SOL violations and operating reserves, or 3) the status, real power flow or reactive power flow of Bulk Electric System elements critical to assessing one IROL or system restoration and operating reserves.	
IRO-002-1	R7.	Each Reliability Coordinator shall have adequate analysis tools such as state estimation, pre- and post-contingency analysis capabilities (thermal, stability, and voltage), and wide-area overview displays.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing all pre-contingency flows, 2) analysis tools capable of assessing all post-contingency flows, or 3) all necessary wide-area overview displays exist.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing the majority of pre-contingency flows, 2) analysis tools capable of assessing the majority of post-contingency flows, or 3) the majority of necessary wide-area overview displays exist.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing a minority of pre-contingency flows, 2) analysis tools capable of assessing a minority of post-contingency flows, or 3) a minority of necessary wide-area overview displays exist.	The Reliability Coordinator failed to demonstrate that it has: 1) analysis tools capable of assessing any pre-contingency flows, 2) analysis tools capable of assessing any post-contingency flows, or 3) any necessary wide-area overview displays exist.
IRO-002-1	R8.	Each Reliability Coordinator shall continuously monitor its Reliability Coordinator Area. Each Reliability	The Reliability Coordinator failed to demonstrate that:	The Reliability Coordinator failed to demonstrate that:	The Reliability Coordinator failed to demonstrate that:	The Reliability Coordinator failed to demonstrate that it

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Coordinator shall have provisions for backup facilities that shall be exercised if the main monitoring system is unavailable. Each Reliability Coordinator shall ensure SOL and IROL monitoring and derivations continue if the main monitoring system is unavailable.	1) it or a delegated entity monitored SOLs when the main monitoring system was unavailable or 2) it has provisions to monitor SOLs when the main monitoring system is not available.	1) it or a delegated entity monitored one IROL when the main monitoring system was unavailable or 2) it has provisions to monitor one IROL when the main monitoring system is not available.	1) it or a delegated entity monitored two or more IROLs when the main monitoring system was unavailable, 2) it or a delegated entity monitored SOLs and one IROL when the main monitoring system was unavailable 3) it has provisions to monitor two or more IROLs when the main monitoring system is not available, or 4) it has provisions to monitor SOLs and one IROL when the main monitoring system was unavailable.	continuously monitored its Reliability Authority Area.
IRO-002-1	R9.	Each Reliability Coordinator shall control its Reliability Coordinator analysis tools, including approvals for planned maintenance. Each Reliability Coordinator shall have procedures in place to mitigate the effects of analysis tool outages.	Reliability Coordinator has approval rights for planned maintenance outages of analysis tools but does not have approval rights for work on analysis tools that creates a greater	Reliability Coordinator has approval rights for planned maintenance but does not have plans to mitigate the effects of outages of the analysis tools.	Reliability Coordinator has approval rights for planned maintenance but does not have plans to mitigate the effects of outages of the analysis tools and does not have approval rights for	Reliability Coordinator approval is not required for planned maintenance.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			risk of an unplanned outage of the tools.		work on analysis tools that creates a greater risk of an unplanned outage of the tools.	
IRO-003-2	R1.	Each Reliability Coordinator shall monitor all Bulk Electric System facilities, which may include sub-transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.	N/A	N/A	The Reliability Coordinator failed to monitor **all** Bulk Electric System facilities, which may include sub-transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.	The Reliability Coordinator failed to monitor Bulk Electric System facilities, which may include sub-transmission information, within adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.
IRO-003-2	R2.	Each Reliability Coordinator shall know the current status of all critical	N/A	N/A	The Reliability Coordinator failed	The Reliability Coordinator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		facilities whose failure, degradation or disconnection could result in an SOL or IROL violation. Reliability Coordinators shall also know the status of any facilities that may be required to assist area restoration objectives.			to know either the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation or the status of any facilities that may be required to assist area restoration objectives.	know the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation and the status of any facilities that may be required to assist area restoration objectives.
IRO-004-1	R1.	Each Reliability Coordinator shall conduct next-day reliability analyses for its Reliability Coordinator Area to ensure that the Bulk Electric System can be operated reliably in anticipated normal and Contingency event conditions. The Reliability Coordinator shall conduct Contingency analysis studies to identify potential interface and other SOL and IROL violations, including overloaded transmission lines and transformers, voltage and stability limits, etc.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for one (1) day during a calendar month.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for two (2) to three (3) days during a calendar month.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for four (4) to five (5) days during a calendar month.	The Reliability Coordinator failed to conduct next-day reliability analyses or contingency analysis for its Reliability Coordinator Area for more than five (5) days during a calendar month.
IRO-004-1	R2.	Each Reliability Coordinator shall pay particular attention to parallel flows to ensure one Reliability Coordinator Area does not place an unacceptable or undue Burden on an adjacent Reliability Coordinator Area.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor parallel flows to ensure one Reliability Coordinator Area does not place an unacceptable or undue Burden on an adjacent

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Reliability Coordinator Area.
IRO-004-1	R3.	Each Reliability Coordinator shall, in conjunction with its Transmission Operators and Balancing Authorities, develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for one (1) day during a calendar month.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for two (2) to three (3) days during a calendar month.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for four (4) to five (5) days during a calendar month.	The Reliability Coordinator, in conjunction with its Transmission Operators and Balancing Authorities, failed to develop action plans that may be required, including reconfiguration of the transmission system, re-dispatching of generation, reduction or curtailment of Interchange Transactions, or reducing load to return transmission loading to within acceptable SOLs or IROLs for more than five (5) days during a calendar month.
IRO-004-1	R4.	Each Transmission Operator, Balancing Authority, Transmission Owner, Generator Owner, Generator Operator, and Load-Serving Entity in the Reliability Coordinator Area shall provide information required for system studies, such as critical facility	The responsible entity in the Reliability Coordinator Area provided the information required for system	The responsible entity in the Reliability Coordinator Area provided the information required for system	The responsible entity in the Reliability Coordinator Area provided the information required for system	The responsible entity in the Reliability Coordinator Area provided the information required for system studies, such as critical facility

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		status, Load, generation, operating reserve projections, and known Interchange Transactions. This information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for one (1) day during a calendar month.	studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for two (2) to three (3) days during a calendar month.	studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for four (4) to five (5) days during a calendar month.	status, Load, generation, operating reserve projections, and known Interchange Transactions, but said information was provided after the required time as stated in IRO-004-1 R4 for more than five (5) days during a calendar month.
IRO-004-1	R5.	Each Reliability Coordinator shall share the results of its system studies, when conditions warrant or upon request, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area. The Reliability Coordinator shall make study results available no later than 1500 Central Standard Time for the Eastern Interconnection and 1500 Pacific Standard Time for the Western Interconnection, unless circumstances warrant otherwise.	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for one (1) day	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for two (2) to three	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for four (4) to five	The Reliability Coordinator failed to share the results of its system studies, when conditions warranted or was requested, with other Reliability Coordinators and with Transmission Operators, Balancing Authorities, and Transmission Service Providers within its Reliability Coordinator Area for more than five (5) days during a calendar month.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			during a calendar month.	(3) days during a calendar month.	(5) days during a calendar month.	
IRO-004-1	R6.	If the results of these studies indicate potential SOL or IROL violations, the Reliability Coordinator shall direct its Transmission Operators, Balancing Authorities and Transmission Service Providers to take any necessary action the Reliability Coordinator deems appropriate to address the potential SOL or IROL violation.	The Reliability Coordinator failed to direct action to address a potential SOL or IROL violation on one (1) occasion during a calendar month.	The Reliability Coordinator failed to direct action to address a potential SOL or IROL violation on two (2) to three (3) occasions during a calendar month.	The reliability Coordinator failed to direct action to address a potential SOL or IROL violation on four (4) to five (5) occasions during a calendar month.	The Reliability Coordinator failed to direct action to address a potential SOL or IROL violation on more than five (5) occasions during a calendar month.
IRO-004-1	R7.	Each Transmission Operator, Balancing Authority, and Transmission Service Provider shall comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on one (1) occasion during a calendar month.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on two (2) to three (3) occasions during a calendar month.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on four (4) to five (5) occasions during a calendar month.	The responsible entity failed to comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events on more than five (5) occasions during a calendar month.
IRO-005-2	R1.	Each Reliability Coordinator shall monitor its Reliability Coordinator Area parameters, including but not limited to the following:	The Reliability Coordinator failed to monitor one (1) of the elements listed in IRO-005-2 R1.1 through R1.10.	The Reliability Coordinator failed to monitor two (2) of the elements listed in IRO-005-2 R1.1 through R1.10.	The Reliability Coordinator failed to monitor three (3) of the elements listed in IRO-005-2 R1.1 through R1.10.	The Reliability Coordinator failed to monitor more than three (3) of the elements listed in IRO-005-2 R1.1 through R1.10.
IRO-005-2	R1.1.	Current status of Bulk Electric System elements (transmission or generation	N/A	N/A	N/A	The Reliability Coordinator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		including critical auxiliaries such as Automatic Voltage Regulators and Special Protection Systems) and system loading.				monitor the current status of Bulk Electric System elements (transmission or generation including critical auxiliaries such as Automatic Voltage Regulators and Special Protection Systems) and system loading.
IRO-005-2	R1.2.	Current pre-contingency element conditions (voltage, thermal, or stability), including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current pre-contingency element conditions (voltage, thermal, or stability); including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.
IRO-005-2	R1.3.	Current post-contingency element conditions (voltage, thermal, or stability), including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current post-contingency element conditions (voltage, thermal, or stability); including any applicable mitigation plans to alleviate SOL or IROL violations, including the plan's viability and scope.
IRO-005-2	R1.4.	System real and reactive reserves	N/A	N/A	N/A	The Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(actual versus required).				Coordinator failed to monitor system real and reactive reserves (actual versus required).
IRO-005-2	R1.5.	Capacity and energy adequacy conditions.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor capacity and energy adequacy conditions.
IRO-005-2	R1.6.	Current ACE for all its Balancing Authorities.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current ACE for all its Balancing Authorities.
IRO-005-2	R1.7.	Current local or Transmission Loading Relief procedures in effect.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor current local or Transmission Loading Relief procedures in effect.
IRO-005-2	R1.8.	Planned generation dispatches.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor planned generation dispatches.
IRO-005-2	R1.9.	Planned transmission or generation outages.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor planned transmission or generation outages.
IRO-005-2	R1.10.	Contingency events.	N/A	N/A	N/A	The Reliability Coordinator failed to monitor contingency events.
IRO-005-2	R2.	Each Reliability Coordinator shall be aware of all Interchange Transactions	N/A	N/A	The Reliability Coordinator was	The Reliability Coordinator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that wheel through, source, or sink in its Reliability Coordinator Area, and make that Interchange Transaction information available to all Reliability Coordinators in the Interconnection.			aware of all Interchange Transactions that wheeled through, sourced or sinked in its Reliability Coordinator Area, but failed to make that Interchange Transaction information available to all Reliability Coordinators in the Interconnection.	be aware of all Interchange Transactions that wheeled through, sourced or sinked in its Reliability Coordinator Area, and failed to make that Interchange Transaction information available to all Reliability Coordinators in the Interconnection.
IRO-005-2	R3.	As portions of the transmission system approach or exceed SOLs or IROLs, the Reliability Coordinator shall work with its Transmission Operators and Balancing Authorities to evaluate and assess any additional Interchange Schedules that would violate those limits. If a potential or actual IROL violation cannot be avoided through proactive intervention, the Reliability Coordinator shall initiate control actions or emergency procedures to relieve the violation without delay, and no longer than 30 minutes. The Reliability Coordinator shall ensure all resources, including load shedding, are available to address a potential or actual IROL violation.	N/A	The Reliability Coordinator worked with its Transmission Operators and Balancing Authorities, as portions of the transmission system approached or exceeded SOLs or IROLs, to evaluate and assess any additional Interchange Schedules that would violate those limits and initiated control actions or emergency procedures to	The Reliability Coordinator worked with its Transmission Operators and Balancing Authorities, as portions of the transmission system approached or exceeded SOLs or IROLs, to evaluate and assess any additional Interchange Schedules that would violate those limits and ensured all resources, including load shedding, were	The Reliability Coordinator failed to work with its Transmission Operators and Balancing Authorities, as portions of the transmission system approached or exceeded SOLs or IROLs, to evaluate and assess any additional Interchange Schedules that would violate those limits and failed to initiate control actions or emergency procedures to relieve the violation within 30 minutes.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				relieve the violation within 30 minutes, but failed to ensure all resources, including load shedding, were available to address a potential or actual IROL violation.	available to address a potential or actual IROL violation, but failed to initiate control actions or emergency procedures to relieve the violation within 30 minutes.	
IRO-005-2	R4.	Each Reliability Coordinator shall monitor its Balancing Authorities' parameters to ensure that the required amount of operating reserves is provided and available as required to meet the Control Performance Standard and Disturbance Control Standard requirements. If necessary, the Reliability Coordinator shall direct the Balancing Authorities in the Reliability Coordinator Area to arrange for assistance from neighboring Balancing Authorities. The Reliability Coordinator shall issue Energy Emergency Alerts as needed and at the request of its Balancing Authorities and Load-Serving Entities.	N/A	The Reliability Coordinator failed to direct the Balancing Authorities in the Reliability Coordinator Area to arrange for assistance from neighboring Balancing Authorities.	The Reliability Coordinator failed to issue Energy Emergency Alerts as needed and at the request of its Balancing Authorities and Load-Serving Entities.	The Reliability Coordinator failed to monitor its Balancing Authorities' parameters to ensure that the required amount of operating reserves was provided and available as required to meet the Control Performance Standard and Disturbance Control Standard requirements.
IRO-005-2	R5.	Each Reliability Coordinator shall identify the cause of any potential or actual SOL or IROL violations. The Reliability Coordinator shall initiate the control action or emergency procedure to relieve the potential or actual IROL violation without delay, and no longer than 30 minutes. The Reliability Coordinator shall be able to utilize all resources, including load	N/A	N/A	The Reliability Coordinator identified the cause of a potential or actual SOL or IROL violation, but failed to initiate a control action or emergency procedure to relieve	The Reliability Coordinator failed to identify the cause of a potential or actual SOL or IROL violation and failed to initiate a control action or emergency procedure to relieve the potential or actual

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shedding, to address an IROL violation.			the potential or actual IROL violation within 30 minutes.	IROL violation.
IRO-005-2	R6.	Each Reliability Coordinator shall ensure its Transmission Operators and Balancing Authorities are aware of Geo-Magnetic Disturbance (GMD) forecast information and assist as needed in the development of any required response plans.	N/A	N/A	The Reliability Coordinator ensured its Transmission Operators and Balancing Authorities were aware of Geo-Magnetic Disturbance (GMD) forecast information, but failed to assist, when needed, in the development of any required response plans.	The Reliability Coordinator failed to ensure its Transmission Operators and Balancing Authorities were aware of Geo-Magnetic Disturbance (GMD) forecast information.
IRO-005-2	R7.	The Reliability Coordinator shall disseminate information within its Reliability Coordinator Area, as required.	N/A	N/A	N/A	The Reliability Coordinator failed to disseminate information within its Reliability Coordinator Area, when required.
IRO-005-2	R8.	Each Reliability Coordinator shall monitor system frequency and its Balancing Authorities' performance and direct any necessary rebalancing to return to CPS and DCS compliance. The Transmission Operators and Balancing Authorities shall utilize all resources, including firm load	N/A	N/A	The Reliability Coordinator monitored system frequency and its Balancing Authorities' performance but failed to direct any	The Reliability Coordinator failed to monitor system frequency and its Balancing Authorities' performance and direct any necessary rebalancing to return

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shedding, as directed by its Reliability Coordinator to relieve the emergent condition.			necessary rebalancing to return to CPS and DCS compliance.	to CPS and DCS compliance or the responsible entity failed to utilize all resources, including firm load shedding, as directed by its Reliability Coordinator to relieve the emergent condition.
IRO-005-2	R9.	The Reliability Coordinator shall coordinate with Transmission Operators, Balancing Authorities, and Generator Operators as needed to develop and implement action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations. The Reliability Coordinator shall coordinate pending generation and transmission maintenance outages with Transmission Operators, Balancing Authorities, and Generator Operators as needed in both the real-time and next-day reliability analysis timeframes.	N/A	The Reliability Coordinator coordinated with Transmission Operators, Balancing Authorities, and Generator Operators, as needed, to develop action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations but failed to implement said plans, or the Reliability Coordinator coordinated pending generation and transmission maintenance outages with Transmission	The Reliability Coordinator failed to coordinate with Transmission Operators, Balancing Authorities, and Generator Operators as needed to develop and implement action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations, or the Reliability Coordinator failed to coordinate pending generation and transmission maintenance outages with Transmission Operators,	The Reliability Coordinator failed to coordinate with Transmission Operators, Balancing Authorities, and Generator Operators as needed to develop and implement action plans to mitigate potential or actual SOL, IROL, CPS, or DCS violations and the Reliability Coordinator failed to coordinate pending generation and transmission maintenance outages with Transmission Operators, Balancing Authorities, and Generator Operators as needed in both the real-time and next-day

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Operators, Balancing Authorities, and Generator Operators as needed in the real-time reliability analysis timeframe but failed to coordinate pending generation and transmission maintenance outages in the next-day reliability analysis timeframe.	Balancing Authorities, and Generator Operators as needed in both the real-time and next-day reliability analysis timeframes.	reliability analysis timeframes.
IRO-005-2	R10.	As necessary, the Reliability Coordinator shall assist the Balancing Authorities in its Reliability Coordinator Area in arranging for assistance from neighboring Reliability Coordinator Areas or Balancing Authorities.	N/A	N/A	N/A	The Reliability Coordinator failed to assist the Balancing Authorities in its Reliability Coordinator Area in arranging for assistance from neighboring Reliability Coordinator Areas or Balancing Authorities, when necessary.
IRO-005-2	R11.	The Reliability Coordinator shall identify sources of large Area Control Errors that may be contributing to Frequency Error, Time Error, or Inadvertent Interchange and shall discuss corrective actions with the appropriate Balancing Authority. The	N/A	The Reliability Coordinator identified sources of large Area Control Errors that were contributing to Frequency Error,	The Reliability Coordinator identified sources of large Area Control Errors that were contributing to Frequency Error,	The Reliability Coordinator failed to identify sources of large Area Control Errors that were contributing to Frequency Error,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinator shall direct its Balancing Authority to comply with CPS and DCS.		Time Error, or Inadvertent Interchange and discussed corrective actions with the appropriate Balancing Authority but failed to direct the Balancing Authority to comply with CPS and DCS.	Time Error, or Inadvertent Interchange but failed to discuss corrective actions with the appropriate Balancing Authority.	Time Error, or Inadvertent Interchange.
IRO-005-2	R12.	Whenever a Special Protection System that may have an inter-Balancing Authority, or inter-Transmission Operator impact (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation) is armed, the Reliability Coordinators shall be aware of the impact of the operation of that Special Protection System on inter-area flows. The Transmission Operator shall immediately inform the Reliability Coordinator of the status of the Special Protection System including any degradation or potential failure to operate as expected.	N/A	N/A	N/A	The Reliability Coordinator failed to be aware of the impact on inter-area flows of an inter-Balancing Authority or inter-Transmission Operator, following the operation of a Special Protection System that is armed (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation), or the Transmission Operator failed to immediately inform the Reliability Coordinator of the status of the Special

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Protection System including any degradation or potential failure to operate as expected.
IRO-005-2	R13.	Each Reliability Coordinator shall ensure that all Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities operate to prevent the likelihood that a disturbance, action, or non-action in its Reliability Coordinator Area will result in a SOL or IROL violation in another area of the Interconnection. In instances where there is a difference in derived limits, the Reliability Coordinator and its Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall always operate the Bulk Electric System to the most limiting parameter.	N/A	N/A	N/A	The Reliability Coordinator failed to shall ensure that all Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities operated to prevent the likelihood that a disturbance, action, or non-action in its Reliability Coordinator Area could result in a SOL or IROL violation in another area of the Interconnection or the responsible entity failed to operate the Bulk Electric System to the most limiting parameter in instances where there was a difference in derived limits..
IRO-005-2	R14.	Each Reliability Coordinator shall make known to Transmission Service	N/A	N/A	N/A	The Reliability Coordinator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Providers within its Reliability Coordinator Area, SOLs or IROLs within its wide-area view. The Transmission Service Providers shall respect these SOLs or IROLs in accordance with filed tariffs and regional Total Transfer Calculation and Available Transfer Calculation processes.				make known to Transmission Service Providers within its Reliability Coordinator Area, SOLs or IROLs within its wide-area view, or the Transmission Service Providers failed to respect these SOLs or IROLs in accordance with filed tariffs and regional Total Transfer Calculation and Available Transfer Calculation processes.
IRO-005-2	R15.	Each Reliability Coordinator who foresees a transmission problem (such as an SOL or IROL violation, loss of reactive reserves, etc.) within its Reliability Coordinator Area shall issue an alert to all impacted Transmission Operators and Balancing Authorities in its Reliability Coordinator Area without delay. The receiving Reliability Coordinator shall disseminate this information to its impacted Transmission Operators and Balancing Authorities. The Reliability Coordinator shall notify all impacted Transmission Operators, Balancing Authorities, when the transmission problem has been mitigated.	N/A	The Reliability Coordinator failed to notify all impacted Transmission Operators, Balancing Authorities, when the transmission problem had been mitigated.	N/A	The Reliability Coordinator who foresaw a transmission problem (such as an SOL or IROL violation, loss of reactive reserves, etc.) within its Reliability Coordinator Area failed to issue an alert to all impacted Transmission Operators and Balancing Authorities in its Reliability Coordinator Area, or the receiving Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Coordinator failed to disseminate this information to its impacted Transmission Operators and Balancing Authorities.
IRO-005-2	R16.	Each Reliability Coordinator shall confirm reliability assessment results and determine the effects within its own and adjacent Reliability Coordinator Areas. The Reliability Coordinator shall discuss options to mitigate potential or actual SOL or IROL violations and take actions as necessary to always act in the best interests of the Interconnection at all times.	N/A	N/A	The Reliability Coordinator confirmed the reliability assessment results and determine the effects within its own and adjacent Reliability Coordinator Areas and discussed options to mitigate potential or actual SOL or IROL violations, but failed to take actions as necessary to always act in the best interests of the Interconnection at all times.	The Reliability Coordinator failed to confirm reliability assessment results and determine the effects within its own and adjacent Reliability Coordinator Areas, or failed to discuss options to mitigate potential or actual SOL or IROL violations and take actions as necessary to always act in the best interests of the Interconnection at all times.
IRO-005-2	R17.	When an IROL or SOL is exceeded, the Reliability Coordinator shall evaluate the local and wide-area impacts, both real-time and post-contingency, and determine if the actions being taken are appropriate and sufficient to return the system to within	N/A	N/A	N/A	The Reliability Coordinator either failed to evaluate the local and wide-area impacts of an IROL or SOL that was exceeded, in either

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		IROL in thirty minutes. If the actions being taken are not appropriate or sufficient, the Reliability Coordinator shall direct the Transmission Operator, Balancing Authority, Generator Operator, or Load-Serving Entity to return the system to within IROL or SOL.				real-time or post-contingency, or the Reliability Coordinator evaluated the local and wide-area impacts of an IROL or SOL that was exceeded, both real-time and post-contingency, and determined that the actions being taken were not appropriate and sufficient to return the system to within IROL in thirty (30) minutes, but failed to direct the Transmission Operator, Balancing Authority, Generator Operator, or Load-Serving Entity to return the system to within IROL or SOL.
IRO-006-4	R1.	A Reliability Coordinator experiencing a potential or actual SOL or IROL violation within its Reliability Coordinator Area shall, with its authority and at its discretion, select one or more procedures to provide transmission loading relief. These procedures can be a "local" (regional, interregional, or sub-regional)	For each TLR in the Eastern Interconnection, the Reliability Coordinator violates one (1) requirement of the applicable Interconnection-wide procedure	For each TLR in the Eastern Interconnection, the Reliability Coordinator violated two (2) to three (3) requirements of the applicable Interconnection-	For each TLR in the Eastern Interconnection, the applicable Reliability Coordinator violated four (4) to five (5) requirements of the applicable	For each TLR in the Eastern Interconnection, the Reliability Coordinator violated six (6) or more of the requirements of the applicable Interconnection-wide procedure.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission loading relief procedure or one of the following Interconnection-wide procedures:		wide procedure	Interconnection-wide procedure	
IRO-006-4	R1.1	The Interconnection-wide Transmission Loading Relief (TLR) procedure for use in the Eastern Interconnection provided in Attachment 1-IRO-006-4. The TLR procedure alone is an inappropriate and ineffective tool to mitigate an IROL violation due to the time required to implement the procedure. Other acceptable and more effective procedures to mitigate actual IROL violations include: reconfiguration, redispatch, or load shedding.				While attempting to mitigate an existing IROL violation in the Eastern Interconnection, the Reliability Coordinator applied TLR as the sole remedy for an existing IROL violation.
IRO-006-4	R1.2	The Interconnection-wide transmission loading relief procedure for use in the Western Interconnection isWECC-IRO-STD-006-0 provided at: ftp://www.nerc.com/pub/sys/all_updl/standards/rrs/IRO-STD-006-0_17Jan07.pdf.				While attempting to mitigate an existing constraint in the Western Interconnection using the "WSCC Unscheduled Flow Mitigation Plan", the Reliability Coordinator did not follow the procedure correctly.
IRO-006-4	R1.3	The Interconnection-wide transmission loading relief procedure for use in ERCOT is				While attempting to mitigate an existing constraint in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		provided as Section 7 of the ERCOT Protocols, posted at: http://www.ercot.com/mktrules/protocols/current.html				ERCOT using Section 7 of the ERCOT Protocols, the Reliability Coordinator did not follow the procedure correctly.
IRO-006-4	R2	The Reliability Coordinator shall only use local transmission loading relief or congestion management procedures to which the Transmission Operator experiencing the potential or actual SOL or IROL violation is a party.	N/A	N/A	N/A	A Reliability Coordinator implemented local transmission loading relief or congestion management procedures to relieve congestion but the Transmission Operator experiencing the congestion was not a party to those procedure
IRO-006-4	R3	Each Reliability Coordinator with a relief obligation from an Interconnection-wide procedure shall follow the curtailments as directed by the Interconnection-wide procedure. A Reliability Coordinator desiring to use a local procedure as a substitute for curtailments as directed by the Interconnection-wide procedure shall obtain prior approval of the local procedure from the ERO.	N/A	N/A	N/A	A Reliability Coordinator implemented local transmission loading relief or congestion management procedures as a substitute for curtailment as directed by the Interconnection-wide procedure but

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the local procedure had not received prior approval from the ERO
IRO-006-4	R4	When Interconnection-wide procedures are implemented to curtail Interchange Transactions that cross an Interconnection boundary, each Reliability Coordinator shall comply with the provisions of the Interconnection-wide procedure.	When requested to curtail an Interchange Transaction that crosses an Interconnection boundary utilizing an Interconnection-wide procedure, the responding Reliability Coordinator did not comply with the provisions of the Interconnection-wide procedure as requested by the initiating Reliability Coordinator	N/A	N/A	N/A
IRO-006-4	R5	During the implementation of relief procedures, and up to the point that emergency action is necessary, Reliability Coordinators and Balancing Authorities shall comply with applicable Interchange scheduling standards.	The Reliability Coordinators or Balancing Authorities did not comply with applicable Interchange	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			scheduling standards during the implementation of the relief procedures, up to the point emergency action is necessary			
IRO-014-1	R1.	The Reliability Coordinator shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability. These Operating Procedures, Processes, or Plans shall address Scenarios that affect other Reliability Coordinator Areas as well as those developed in coordination with other Reliability Coordinators.	N/A	N/A	The Reliability Coordinator has Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability, but failed to address Scenarios that affect other Reliability Coordinator Areas.	The Reliability Coordinator failed to have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability.
IRO-014-1	R1.1.	These Operating Procedures, Processes, or Plans shall collectively address, as a minimum, the following:	The Reliability Coordinator failed to include one of	The Reliability Coordinator failed to include two of	The Reliability Coordinator failed to include more	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in there Operating Procedures, Processes, or Plans.	the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in there Operating Procedures, Processes, or Plans.	than two of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in there Operating Procedures, Processes, or Plans.	
IRO-014-1	R1.1.1.	Communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to address communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.2.	Energy and capacity shortages.	N/A	N/A	N/A	The Reliability Coordinator failed to address energy and capacity shortages in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.3.	Planned or unplanned outage information.	N/A	N/A	N/A	The Reliability Coordinator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						address planned or unplanned outage information in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.4.	Voltage control, including the coordination of reactive resources for voltage control.	N/A	N/A	N/A	The Reliability Coordinator failed to address voltage control, including the coordination of reactive resources for voltage control in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.5.	Coordination of information exchange to support reliability assessments.	N/A	N/A	N/A	The Reliability Coordinator failed to address the coordination of information exchange to support reliability assessments in its Operating Procedure, Process or Plan.
IRO-014-1	R1.1.6.	Authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas.	N/A	N/A	N/A	The Reliability Coordinator failed to address authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas in its Operating Procedure, Process or Plan.
IRO-014-1	R2.	Each Reliability Coordinator's	N/A	N/A	N/A	The Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operating Procedure, Process, or Plan that requires one or more other Reliability Coordinators to take action (e.g., make notifications, exchange information, or coordinate actions) shall be:				Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R2.1 or R2.2.
IRO-014-1	R2.1.	Agreed to by all the Reliability Coordinators required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not agreed to by all the Reliability Coordinators required to take the indicated action(s).
IRO-014-1	R2.2.	Distributed to all Reliability Coordinators that are required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not distributed to all Reliability Coordinators that are required to take the indicated action(s).
IRO-014-1	R3.	A Reliability Coordinator's Operating Procedures, Processes, or Plans developed to support a Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan shall include:	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R3.1 or R3.2.
IRO-014-1	R3.1.	A reference to the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to reference the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R3.2.	The agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to include the agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R4.	Each of the Operating Procedures, Processes, and Plans addressed in Reliability Standard IRO-014 Requirement 1 and Requirement 3 shall:	N/A	N/A	N/A	The Reliability Coordinator developed an Operating Procedure, Process, or Plan in accordance with IRO-014 Requirement 1 and Requirement 3, but failed to comply with one of the elements listed in IRO-014-1 R4.1 through R4.3.
IRO-014-1	R4.1.	Include version control number or date	N/A	N/A	N/A	The Reliability Operator failed to include the version control number or date in its Operating

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Procedure, Process, or Plan.
IRO-014-1	R4.2.	Include a distribution list.	N/A	N/A	N/A	The Reliability Operator failed to include a distribution list in its Operating Procedure, Process, or Plan.
IRO-014-1	R4.3.	Be reviewed, at least once every three years, and updated if needed.	N/A	N/A	N/A	The Reliability Operator failed to review, at least once every three years, and update if needed, its Operating Procedure, Process, or Plan.
IRO-015-1	R1.	The Reliability Coordinator shall follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators but no adverse reliability impacts resulted from the incident.	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators and adverse reliability impacts resulted from the incident.
IRO-015-1	R1.1.	The Reliability Coordinator shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator	N/A	The Reliability Coordinator failed to make notifications to other Reliability	N/A	The Reliability Coordinator failed to make notifications to other Reliability Coordinators of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Areas.		Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas but no adverse reliability impacts resulted from the incident.		conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas and adverse reliability impacts resulted from the incident.
IRO-015-1	R2.	The Reliability Coordinator shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.
IRO-015-1	R2.1.	The frequency of these conference calls shall be agreed upon by all involved Reliability Coordinators and shall be at least weekly.	N/A	N/A	N/A	The Reliability Operator failed to participate in the assessment of the need and frequency of conference calls with other Reliability Operators.
IRO-015-1	R3.	The Reliability Coordinator shall provide reliability-related information as requested by other Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to provide reliability-related information as requested by other Reliability Coordinators.
IRO-016-1	R1.	The Reliability Coordinator that	The Reliability	N/A	N/A	The Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.	Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators, contacted the other Reliability Coordinator(s) to confirm that there was a problem, discussed options and decided upon a solution to prevent or resolve the identified problem, but failed to have evidence that it coordinated with other Reliability Coordinators.			Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators failed to contact the other Reliability Coordinator(s) to confirm that there was a problem, discuss options and decide upon a solution to prevent or resolve the identified problem.
IRO-016-1	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.	The responsible entity agreed on the problem and the actions to take to prevent or mitigate the system condition, implemented the agreed-upon solution, but failed to notify the involved Reliability	N/A	N/A	The responsible entity agreed on the problem and the actions to take to prevent or mitigate the system condition, but failed to implement the agreed-upon solution.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Coordinators of the action(s) taken.			
IRO-016-1	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.).	N/A	N/A	N/A	The involved Reliability Coordinators could not agree on the problem(s), but a Reliability Coordinator failed to re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
IRO-016-1	R1.2.1.	If time permits, this re-evaluation shall be done before taking corrective actions.	N/A	N/A	N/A	The Reliability Coordinator failed to re-evaluate the problem prior to taking corrective actions, during periods when time was not an issue.
IRO-016-1	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.	N/A	N/A	N/A	The Reliability Coordinator failed to operate as though the problem(s) exist(s) until the conflicting system status was resolved, during periods when time was an issue.
IRO-016-1	R1.3.	If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.	N/A	N/A	N/A	The Reliability Coordinator implemented a solution other than the most conservative solution, when

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						agreement on the solution could not be reached.
IRO-016-1	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.	N/A	N/A	N/A	The Reliability Coordinator failed to 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.

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-006-0.1	R1.	Each Transmission Service Provider shall document its procedure on the use of Capacity Benefit Margin (CBM) (scheduling of energy against a CBM reservation). The procedure shall include the following three components:	The Transmission Service Provider documented its procedure on the use of Capacity Benefit Margin (CBM) but failed to include one (1) of the components as specified in R1.1, R1.2 or R1.3.	The Transmission Service Provider documented its procedure on the use of Capacity Benefit Margin (CBM) but failed to include two (2) of the components as specified in R1.1, R1.2 or R1.3.	The Transmission Service Provider documented its procedure on the use of Capacity Benefit Margin (CBM) but failed to include three (3) of the components as specified in R1.1, R1.2 or R1.3.	The Transmission Service Provider failed to document its procedure on the use of Capacity Benefit Margin (CBM).
MOD-006-0.1	R1.1.	Require that CBM be used only after the following steps have been taken (as time permits): all non-firm sales have been terminated, Direct-Control Load Management has been implemented, and customer interruptible demands have been interrupted. CBM may be used to reestablish Operating Reserves.	N/A	The Transmission Service Provider required that CBM be used only after all non-firm sales have been terminated and Direct-Control Load Management has been implemented but failed to include customer interruptible demands that have been interrupted.	The Transmission Service Provider required that CBM be used only after all non-firm sales have been terminated but failed to include Direct-Control Load Management has been implemented and customer interruptible demands that have been interrupted.	The Transmission Service Provider failed to require that CBM be used only after all non-firm sales have been terminated, Direct-Control Load Management has been implemented and customer interruptible demands that have been interrupted.
MOD-006-0.1	R1.2.	Require that CBM shall only be used if the Load-Serving Entity calling for its use is experiencing a generation deficiency and its Transmission Service Provider is also experiencing Transmission Constraints relative to imports of energy on its transmission	N/A	The Transmission Service Provider required that CBM shall only be used if the Load-Serving Entity calling for its use is	N/A	The Transmission Service Provider failed to require that CBM shall only be used if the Load-Serving Entity calling for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system.		experiencing a generation deficiency but failed to require that CBM shall only be used if its Transmission Service Provider is also experiencing Transmission Constraints relative to imports of energy on its transmission system.		its use is experiencing a generation deficiency and its Transmission Service Provider is also experiencing Transmission Constraints relative to imports of energy on its transmission system.
MOD-006-0.1	R1.3.	Describe the conditions under which CBM may be available as Non-Firm Transmission Service.	N/A	N/A	N/A	The Transmission Service Provider has failed to describe the conditions under which CBM may be available as Non-Firm Transmission Service.
MOD-006-0.1	R2.	Each Transmission Service Provider shall make its CBM use procedure available on a web site accessible by the Regional Reliability Organizations, NERC, and transmission users.	The Transmission Service Provider has demonstrated the procedure is available on the Web but is deficient with minor details.	N/A	N/A	The Transmission Service Provider has failed to provide the procedure on the Web as directed by the requirement.
MOD-007-0	R1.	Each Transmission Service Provider that uses CBM shall report (to the Regional Reliability Organization,	N/A	Each Transmission Service Provider that uses CBM	N/A	Each Transmission Service Provider that uses CBM

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		NERC and the transmission users) the use of CBM by the Load-Serving Entities' Loads on its system, except for CBM sales as Non-Firm Transmission Service. (This use of CBM shall be consistent with the Transmission Service Provider's procedure for use of CBM.)		reported (to the Regional Reliability Organization, NERC and the transmission users) the use of CBM by the Load-Serving Entities' Loads on its system but failed to use CBM that is consistent with the Transmission Service Provider's procedure for use of CBM.		failed to report (to the Regional Reliability Organization, NERC and the transmission users) the use of CBM by the Load-Serving Entities' Loads on its system.
MOD-007-0	R2.	The Transmission Service Provider shall post the following three items within 15 calendar days after the use of CBM for an Energy Emergency. This posting shall be on a web site accessible by the Regional Reliability Organizations, NERC, and transmission users.	The Transmission Service Provider that uses CBM for an Energy Emergency complied with the posting of the 3 required items but is deficient regarding minor details.	The Transmission Service Provider that uses CBM for an Energy Emergency complied with the posting but is deficient regarding one of the 3 requirements.	The Transmission Service Provider that uses CBM for an Energy Emergency complied with the posting but is deficient regarding two of the 3 requirements.	The Transmission Service Provider that uses CBM for an Energy Emergency did not comply with the posting as required.
MOD-007-0	R2.1.	Circumstances.	The Transmission Service Provider posted the circumstance more than 15 but less than or equal to 20 calendar days after the use of CBM for	The Transmission Service Provider posted the circumstance more than 20 but less than or equal to 25 calendar days after the use of CBM for	The Transmission Service Provider posted the circumstance more than 25 but less than or equal to 30 calendar days after the use of CBM for	The Transmission Service Provider failed to post the circumstance more than 30 calendar days after the use of CBM for an Energy Emergency.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			an Energy Emergency.	an Energy Emergency.	an Energy Emergency.	
MOD-007-0	R2.2.	Duration.	The Transmission Service Provider posted the duration more than 15 but less than or equal to 20 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the duration more than 20 but less than or equal to 25 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the duration more than 25 but less than or equal to 30 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider failed to post the duration more than 30 calendar days after the use of CBM for an Energy Emergency.
MOD-007-0	R2.3.	Amount of CBM used.	The Transmission Service Provider posted the amount of CBM used more than 15 but less than or equal to 20 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the amount of CBM used more than 20 but less than or equal to 25 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider posted the amount of CBM used more than 25 but less than or equal to 30 calendar days after the use of CBM for an Energy Emergency.	The Transmission Service Provider failed to post the amount of CBM used more than 30 calendar days after the use of CBM for an Energy Emergency.
MOD-010-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics, system data, and existing and future Interchange	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to 50% of the appropriate equipment characteristics, system data, and existing and future	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the appropriate equipment characteristics, system data, and existing and future	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1	Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.
MOD-010-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide this steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. If no schedule exists, then these entities shall provide the data on request (30 calendar days).	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to 50% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 30 but less than or equal to 35 calendar days following the request.	OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.	OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 40 but less than or equal to 45 calendar days following the request.	If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide data more than 45 calendar days following the request.
MOD-012-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R1) shall provide appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1	simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.
MOD-012-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R4) shall provide dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. If no schedule exists, then these entities shall provide data on request (30 calendar days).	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1 OR	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 30 but less than or equal to 35 calendar days following the request.	If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.	If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 40 but less than or equal to 45 calendar days following the request.	exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide data more than 45 calendar days following the request.
MOD-016-1.1	R1.	The Planning Authority and Regional Reliability Organization shall have documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses.	N/A	The Planning Authority and Regional Reliability Organization has documentation identifying the scope and details of the actual and forecast data but failed to have documentation identifying the scope data and details for one (1) of the following actual and forecast data to be reported for system modeling and reliability analyses: (a) Demand data,	The Planning Authority and Regional Reliability Organization has documentation identifying the scope and details of the actual and forecast data but failed to have documentation identifying the scope data and details for two (2) of the following actual and forecast data to be reported for system modeling and reliability analyses: (a) Demand data,	The Planning Authority and Regional Reliability Organization has failed to have documentation identifying the scope and details of the actual and forecast data to be reported for system modeling and reliability analyses.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(b) Net Energy for Load data, or (c) controllable DSM data.	(b) Net Energy for Load data, or (c) controllable DSM data.	
MOD-016-1.1	R1.1.	The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.	The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for less than or equal to 25% or the Reliability Standards as specified in R1.1	The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for greater than 25% but less than or equal to 50% of the Reliability Standards as specified in R1.1.	The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for greater than 50% but less than or equal to 75% of the Reliability Standards as specified in R1.1.	The Planning Authority and Regional Reliability Organization failed to ensure that consistent data is supplied for greater than 75% of the Reliability Standards as specified in R1.1. OR The Planning Authority and Regional Reliability Organization failed to stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-016-1.1	R2.	The Regional Reliability Organization shall distribute its documentation required in Requirement 1 and any changes to that documentation, to all Planning Authorities that work within its Region.	N/A	N/A	The Regional Reliability Organization distributed its documentation as specified in R1 but failed to distribute any changes to that documentation, to all Planning Authorities that work within its Region.	The Regional Reliability Organization failed to distribute its documentation as specified in R1 to all Planning Authorities that work within its Region.
MOD-016-1.1	R2.1.	The Regional Reliability Organization shall make this distribution within 30 calendar days of approval.	The Regional Reliability Organization distributed the documentation more than 30 but less than or equal to 37 calendar days following approval.	The Regional Reliability Organization made the distribution more than 37 but less than or equal to 51 calendar days following approval.	The Regional Reliability Organization made the distribution more than 51 but less than or equal to 58 calendar days following approval.	The Regional Reliability Organization failed to make the distribution more than 58 calendar days following approval.
MOD-016-1.1	R3.	The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area.	N/A	N/A	The Planning Authority distributed its documentation as specified in R1 for reporting customer data but failed to distribute any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work	The Planning Authority failed to distribute its documentation as specified in R1 for reporting customer data to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					within its Planning Authority Area.	
MOD-016-1.1	R3.1.	The Planning Authority shall make this distribution within 30 calendar days of approval.	The Planning Authority distributed the documentation more than 30 but less than or equal to 37 calendar days following approval.	The Planning Authority made the distribution more than 37 but less than or equal to 51 calendar days following approval.	The Planning Authority made the distribution more than 51 but less than or equal to 58 calendar days following approval.	The Planning Authority failed to make the distribution more than 58 calendar days following approval
MOD-017-0.1	R1.	The Load-Serving Entity, Planning Authority, and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R 1.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide one of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide two of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide three of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide all of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.
MOD-017-0.1	R1.1.	Integrated hourly demands in megawatts (MW) for the prior year.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide Integrated hourly demands in megawatts (MW) for the prior year on an annual basis.
MOD-017-0.1	R1.2.	Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						failed to provide monthly and annual peak hour actual demands in MW Net Energy for Load in gigawatthours (GWh) for the prior year.
MOD-017-0.1	R1.3.	Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.
MOD-017-0.1	R1.4.	Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, and Resource Planner failed to provide Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-018-0	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or dispersed basis) shall:	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to report one (1) of the items as specified in R1.1, R1.2, or R1.3.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to report two (2) of the items as specified in R1.1, R1.2, or R1.3.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to report all of the items as specified in R1.1, R1.2, and R1.3.
MOD-018-0	R1.1.	Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included.
MOD-018-0	R1.2.	Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to address assumptions, methods, and the manner in which uncertainties are

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						treated in the forecasts of aggregated peak demands and Net Energy for Load.
MOD-018-0	R1.3.	Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1.	N/A	N/A	N/A	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner failed to address items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) as described in the reporting procedures developed for Standard MOD-016-1_R1.
MOD-018-0	R2.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days).	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to report the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Load-Serving Entity, Planning Authority, and Resource Planner more than 30 but less than or equal to 45 calendar days following the request.	Load-Serving Entity, Planning Authority, and Resource Planner more than 45 but less than or equal to 60 calendar days following the request.	Load-Serving Entity, Planning Authority, and Resource Planner more than 60 but less than or equal to 75 calendar days following the request.	Load-Serving Entity, Planning Authority, and Resource Planner more than 75 calendar days following the request.
MOD-019-0.1	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R 1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually less than or equal to 25% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 25% but less than or equal to 50% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 50% but less than or equal to 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R 1.	Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.	Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.	(Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.
MOD-020-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 30 but less than 45 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 45 but less than 60 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 60 but less than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to make known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.
MOD-021-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource	Load-Serving Entity,	Load-Serving Entity,	Load-Serving Entity,	Load-Serving Entity,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed.	Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how one (1) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how two (2) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how three (3) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	Transmission Planner, and Resource Planner's forecasts failed to document how the Demand and energy effects of DSM programs are addressed.
MOD-021-0	R2.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R 1.	N/A	N/A	N/A	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R 1.
MOD-021-0	R3.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days).	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 30 but less than 45 calendar days following the request from NERC.	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 45 but less than 60 calendar days following the request from NERC.	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 60 but less than 75 calendar days following the request from NERC.	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to provide documentation on the treatment of its DSM programs more than 75 calendar days following the request from NERC.

Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-1	R1.	The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt.	The Nuclear Plant Generator Operator did not verify receipt of the proposed NPIR's.	The Nuclear Plant Generator Operator submitted an incomplete proposed NPIR to the applicable transmission entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to some applicable entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to any applicable entities.
NUC-001-1	R2.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements 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.	N/A	N/A	N/A	The Nuclear Plant Generator Operator or the applicable Transmission Entity does not have in effect one or more agreements that include NPIRs and document the implementation of the NPIRs.
NUC-001-1	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	The applicable Transmission Entity incorporated the NPIRs into its planning analyses and identified no areas of concern but it did not	The applicable Transmission Entity incorporated the NPIRs into its planning analyses and identified one or more areas of concern but did not	The applicable Transmission Entity did not incorporate the NPIRs into its planning analyses of the electric system.	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		communicate the results of these analyses to the Nuclear Plant Generator Operator.	communicate these results to the Nuclear Plant Generator Operator.	communicate these results to the Nuclear Plant Generator Operator.		
NUC-001-1	R4.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall:	The applicable Transmission Entity failed to incorporate one or more applicable NPIRs into their operating analyses.	The applicable Transmission Entity failed to incorporate any NPIRs into their operating analyses OR did not inform NPG operator when their ability of assess the operation of the electric system affecting the NPIRs was lost.	The applicable Transmission Entity failed to operate the system to meet the NPIRs	N/A
NUC-001-1	R4.1	Incorporate the NPIRs into their operating analyses of the electric system.	N/A	N/A	N/A	N/A
NUC-001-1	R4.2	Operate the electric system to meet the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-1	R4.3	Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.	N/A	N/A	N/A	N/A
NUC-001-1	R5.	The Nuclear Plant Generator Operator shall operate per the Agreements developed in	The Nuclear Operator failed to operate the plant in accordance with one	The Nuclear Operator failed to operate the plant in accordance with one	The Nuclear Operator failed to operate the plant in accordance with	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		accordance with this standard.	or more of the administrative or training elements within the agreements.	or two of the technical, operations, and maintenance or communication elements within the agreements.	three or more of the technical, operations, and maintenance or communication elements within the agreements.	
NUC-001-1	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.	The Nuclear Operator or Transmission Entity failed to coordinate outages or maintenance activities in accordance with one or more of the administrative elements within the agreements.	The Nuclear Operator or Transmission Entity failed to provide outage or maintenance schedules to the appropriate parties as described in the agreement or on a time period consistent with the agreements.	The Nuclear Operator or Transmission Entity failed to coordinate one or more outages or maintenance activities in accordance the requirements of the agreements.	N/A
NUC-001-1	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	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of actual changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of actual changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that directly impact the	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		electric system to meet the NPIRs.	ability of the electric system to meet the NPIRs.	ability of the electric system to meet the NPIRs.	ability of the electric system to meet the NPIRs.	
NUC-001-1	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.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of proposed changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that directly impacts the ability of the electric system to meet the NPIRs.	N/A
NUC-001-1	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:	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing one or more sub-components of R9.1.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from one to five of the combined sub-components in R9.2, R9.3 and R9.4.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from six to ten of the combined sub-components in R9.2, R9.3 and R9.4.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing eleven or more of the combined sub-components in R9.2, R9.3 and R9.4.
NUC-001-1	R9.1	Administrative elements:				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-1	R9.1.1	Definitions of key terms used in the agreement.				
NUC-001-1	R9.1.2	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.				
NUC-001-1	R9.1.3	A requirement to review the agreement(s) at least every three years.				
NUC-001-1	R9.1.4	A dispute resolution mechanism.				
NUC-001-1	R9.2	Technical requirements and analysis:				
NUC-001-1	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.				
NUC-001-1	R9.2.2	Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.				
NUC-001-1	R9.2.3	Types of planning and operational analyses performed specifically to support the NPIRs,				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		including the frequency of studies and types of Contingencies and scenarios required.				
NUC-001-1	R9.3	Operations and maintenance coordination:				
NUC-001-1	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.				
NUC-001-1	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.				
NUC-001-1	R9.3.3	Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.				
NUC-001-1	R9.3.4	Provisions to address mitigating actions needed				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.				
NUC-001-1	R9.3.5	Provision to consider nuclear plant coping times required by the NPLRs and their relation to the coordination of grid and nuclear plant restoration following a nuclear plant loss of Off-site Power.				
NUC-001-1	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.				
NUC-001-1	R9.3.7	Coordination of the NPIRs with transmission				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system Special Protection Systems and underfrequency and undervoltage load shedding programs.				
NUC-001-1	R9.4	Communications and training:				
NUC-001-1	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.				
NUC-001-1	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.				
NUC-001-1	R9.4.3	Provisions for coordinating investigations of causes				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.				
NUC-001-1	R9.4.4	Provisions for supplying information necessary to report to government agencies, as related to NPIRs.				
NUC-001-1	R9.4.5	Provisions for personnel training, as related to NPIRs.				

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-001-0	R1.	Each Transmission Operator and Balancing Authority shall provide operating personnel with the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	N/A	N/A	The Transmission Operator and Balancing Authority has failed to demonstrate the communication to the operating personnel their responsibility OR their authority to implement real-time actions to ensure a stable and reliable operation of the Bulk Electric System.	The Transmission Operator and Balancing Authority has failed to demonstrate the communication to the operating personnel their responsibility AND authority to implement real-time actions to ensure a stable and reliable operation of the Bulk Electric System.
PER-002-0	R1.	Each Transmission Operator and Balancing Authority shall be staffed with adequately trained operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting 5% or less of its operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting between 5-10% of its operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting 10-15%, inclusive, of its operating personnel.	The applicable entity did not adequately staff and train operating personnel, affecting greater than 15% of its operating personnel.
PER-002-0	R2.	Each Transmission Operator and Balancing Authority shall have a training program for all operating personnel that are in:	Each Transmission Operator and Balancing Authority has produced the training program for more than 75% but less than 100% of their real-time operating personnel.	Each Transmission Operator and Balancing Authority has produced the training program for more than 50% but less than or equal to 75% of their real-time operating personnel.	Each Transmission Operator and Balancing Authority has produced the training program for more than 25% but less than or equal to 50% of their real-time operating personnel.	Each Transmission Operator and Balancing Authority has produced the training program for more than or equal to 0% but less than or equal to 25% of their real-time operating personnel.
PER-002-0	R2.1.	Positions that have the primary responsibility, either directly or through	N/A	N/A	N/A	The Transmission Operator and Balancing Authority

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		communications with others, for the real-time operation of the interconnected Bulk Electric System.				failed to produce training program for their operating personnel.
PER-002-0	R2.2.	Positions directly responsible for complying with NERC standards.	N/A	N/A	N/A	The Transmission Operator and Balancing Authority failed to produce training program for positions directly responsible for complying with NERC Standards.
PER-002-0	R3.	For personnel identified in Requirement R2, the Transmission Operator and Balancing Authority shall provide a training program meeting the following criteria:	The applicable entity did not comply with one of the four required elements.	The applicable entity did not comply with two of the four required elements.	The applicable entity did not comply with three of the four required elements.	The applicable entity did not comply with any of the four required elements.
PER-002-0	R3.1.	A set of training program objectives must be defined, based on NERC and Regional Reliability Organization standards, entity operating procedures, and applicable regulatory requirements. These objectives shall reference the knowledge and competencies needed to apply those standards, procedures, and requirements to normal,	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for less than 25% of the applicable BA and TOP NERC and Regional Reliability Organizations standards, entity	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 25% or more but less than 50% of the applicable BA & TOP NERC and Regional Reliability Organizations	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 50% or more but less than 75% of the applicable BA & TOP NERC and Regional Reliability Organizations	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 75% or more of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		emergency, and restoration conditions for the Transmission Operator and Balancing Authority operating positions.	operating procedures, and regulatory requirements.)	standards, entity operating procedures, and regulatory requirements.)	standards, entity operating procedures, and regulatory requirements.)	operating procedures, and regulatory requirements.)
PER-002-0	R3.2.	The training program must include a plan for the initial and continuing training of Transmission Operator and Balancing Authority operating personnel. That plan shall address knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.
PER-002-0	R3.3.	The training program must include training time for all Transmission Operator and Balancing Authority operating personnel to ensure their operating proficiency.	The responsible entity has produced the training program with more than 75% but less than 100% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 50% but less than or equal to 75% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 25% but less than or equal to 50% of operating personnel provided with training time.	The responsible entity has produced the training program with more than or equal to 0% but less than or equal to 25% of operating personnel provided with training time.
PER-002-0	R3.4.	Training staff must be identified, and the staff must be competent in both knowledge of system operations and instructional capabilities.	N/A	The responsible entity has produced the training program with training staff identified that lacks knowledge of system	The responsible entity has produced the training program with training staff identified that lacks knowledge of system	The responsible entity has produced the training program with no training staff identified.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				operations. OR The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	operations. AND The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	
PER-002-0	R4.	For personnel identified in Requirement R2, each Transmission Operator and Balancing Authority shall provide its operating personnel at least five days per year of training and drills using realistic simulations of system emergencies, in addition to other training required to maintain qualified operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting 5% or less of its operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting between 5-10% of its operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting 10-15%, inclusive, of its operating personnel.	The applicable entity did not provide five days per year of training and drills, as directed by the requirement, affecting greater than 15% of its operating personnel.
PER-003-0	R1.	Each Transmission Operator, Balancing Authority, and Reliability Coordinator shall staff all operating positions that meet both of the following criteria with personnel that are NERC-certified for the applicable functions:	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 0 hours and less 12 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 12 hours and less 36 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 36 hours and less 72 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 72 hours for any operating position for a calendar month.
PER-003-0	R1.1.	Positions that have the primary responsibility,	The responsible entity failed to staff an	The responsible entity failed to staff an	The responsible entity failed to staff an	The responsible entity failed to staff an

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System.	operating position with NERC certified personnel for greater than 0 hours and less 12 hours for any operating position for a calendar month.	operating position with NERC certified personnel for greater than 12 hours and less 36 hours for any operating position for a calendar month.	operating position with NERC certified personnel for greater than 36 hours and less 72 hours for any operating position for a calendar month.	operating position with NERC certified personnel for greater than 72 hours for any operating position for a calendar month.
PER-003-0	R1.2.	Positions directly responsible for complying with NERC standards.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 0 hours and less 12 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 12 hours and less 36 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 36 hours and less 72 hours for any operating position for a calendar month.	The responsible entity failed to staff an operating position with NERC certified personnel for greater than 72 hours for any operating position for a calendar month.
PER-004-1	R1.	Each Reliability Coordinator shall be staffed with adequately trained and NERC-certified Reliability Coordinator operators, 24 hours per day, seven days per week.	N/A	N/A	N/A	The responsible entity has failed to be staffed with adequately trained and NERC-certified Reliability Coordinator operators, 24 hours per day, seven days per week.
PER-004-1	R2.	All Reliability Coordinator operating personnel shall each complete a minimum of five days per year of training and drills using realistic simulations of system emergencies, in addition to other training required to maintain qualified operating personnel.	The Reliability Coordinator's operating personnel completed at least 4 (but less than 5) days of emergency training.	The Reliability Coordinator's operating personnel completed at least 3 (but less than 4) days of emergency training.	The Reliability Coordinator's operating personnel completed at least 2 (but less than 3) days of emergency training.	The Reliability Coordinator's operating personnel completed less than 2 days of emergency training.
PER-004-1	R3.	Reliability Coordinator	Reliability	Reliability	Reliability	Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		operating personnel shall have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	Coordinator personnel have a comprehensive understanding of the interactions with at least 75% and less than 100% of neighboring Reliability Coordinator areas.	Coordinator personnel have a comprehensive understanding of the interactions with 50% or more and less than 75% of neighboring Reliability Coordinator areas.	Coordinator personnel have a comprehensive understanding of the interactions with 25% or more and less than 50% of neighboring Reliability Coordinator areas.	Coordinator personnel have a comprehensive understanding of the interactions less than 25% of neighboring Reliability Coordinator areas.
PER-004-1	R4.	Reliability Coordinator operating personnel shall have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.	Reliability Coordinator operating personnel have an extensive understanding of the operations of more than 75% and less than 100% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.	Reliability Coordinator operating personnel have an extensive understanding of the operations of more than 50% and less than 75% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.	Reliability Coordinator operating personnel have an extensive understanding of the operations of more than 25% and less than 50% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.	Reliability Coordinator operating personnel have an extensive understanding of the operations of less than 25% of all Balancing Authorities, Transmission Operators and Generator Operators in the Reliability Coordinator Area.
PER-004-1	R5.	Reliability Coordinator operating personnel shall place particular attention on SOLs and IROLs and inter-tie facility limits. The Reliability Coordinator shall ensure protocols are in place to allow Reliability Coordinator operating personnel to have the best available information at all times.	Reliability Coordinator has failed to provide its operating personnel with less than 25% of the SOL and IROL limits and for inter-tie facility limits OR the protocols to ensure best available data at all times is not in	Reliability Coordinator has failed to provide its operating personnel with 25% or more and less than 50% of the SOL and IROL limits and for inter-tie facility limits.	Reliability Coordinator has failed to provide its operating personnel with 50% or more and less than 75% of the SOL and IROL limits and for inter-tie facility limits.	Reliability Coordinator has failed to provide its operating personnel with 75% or more of the SOL and IROL limits and for inter-tie facility limits.

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			place.			

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-001-1	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.	N/A	N/A	The responsible entity was familiar with the purpose of protection system schemes applied in its area but failed to be familiar with the limitations of protection system schemes applied in its area.	The responsible entity failed to be familiar with the purpose and limitations of protection system schemes applied in its area.
PRC-001-1	R2.	Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:	N/A	N/A	N/A	The responsible entity failed to notify any reliability entity of relay or equipment failures.
PRC-001-1	R2.1.	If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, but corrective action was taken.	Notification of relay or equipment failure was made to the Transmission Operator and Host Balancing Authority, but corrective action was not taken.	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, and corrective action was not taken.
PRC-001-1	R2.2.	If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing	Notification of relay or equipment failure was made to the Reliability Coordinator and affected Transmission Operators and Balancing	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Authorities, but corrective action was taken.	Authorities, but corrective action was not taken.	Authorities, and corrective action was not taken.
PRC-001-1	R3.	A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.	N/A	N/A	N/A	N/A
PRC-001-1	R3.1.	Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.	The Generator Operator failed to coordinate one new protective system or one protective system change with either its Transmission Operator or its Host Balancing Authority or both.	The Generator Operator failed to coordinate two new protective systems or two protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate three new protective systems or three protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate more than three new protective systems or more than three changes with its Transmission Operator and Host Balancing Authority.
PRC-001-1	R3.2.	Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate one new protective system or one protective system change with either its Transmission Operator or its Host Balancing Authority or both.	The Transmission Operator failed to coordinate two new protective systems or two protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Transmission Operator failed to coordinate three new protective systems or three protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Transmission Operator failed to coordinate more than three new protective systems or more than three system changes with neighboring Transmission Operators and Balancing Authorities.
PRC-001-1	R4.	Each Transmission Operator shall coordinate protection systems on major transmission lines and interconnections with neighboring Generator Operators,	The Transmission Operator failed to coordinate protection systems on major	The Transmission Operator failed to coordinate protection systems on major	The Transmission Operator failed to coordinate protection systems on major	The Transmission Operator failed to coordinate protection systems on major

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Operators, and Balancing Authorities.	transmission lines and interconnections with one of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	transmission lines and interconnections with two of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	transmission lines and interconnections with three of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	transmission lines and interconnections with three or more of its neighboring Generator Operators, Transmission Operators, and Balancing Authorities.
PRC-001-1	R5.	A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the protection systems of others:	N/A	N/A	N/A	The responsible entity failed to coordinate changes in generation, transmission, load or operating conditions that could require changes in the protection systems of others:
PRC-001-1	R5.1.	Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.	N/A	N/A	N/A	The Generator Operator failed to notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.
PRC-001-1	R5.2.	Each Transmission Operator shall notify neighboring Transmission	N/A	N/A	N/A	The Transmission Operator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.				notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.
PRC-001-1	R6.	Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.	N/A	N/A	Notification of a change in status of a Special Protection System was not made to the affected Transmission Operators and Balancing Authorities.	The responsible entity failed to monitor the status of each Special Protection System in its area, and did not notify affected Transmission Operators and Balancing Authorities of each change in status.
PRC-004-1	R1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		procedures developed for Reliability Standard PRC-003 Requirement 1.				
PRC-004-1	R2.	The Generator Owner shall analyze its generator Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed
PRC-004-1	R3.	The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its Regional Reliability Organization, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses and its Corrective Action Plans, but did not provide these according to the Regional Reliability Organization's procedures.	N/A	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses but did not provide its Corrective Action Plans.	The responsible entity did not provide its Regional Reliability Organization with documentation of its Misoperations analyses and did not provide its Corrective Action Plans.
PRC-005-1	R1.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the	N/A	N/A	The responsible entity that owned a transmission Protection System or Generator Owner that owned a generation Protection System failed to have either	The responsible entity that owned a transmission Protection System or Generator Owner that owned a generation Protection System failed to have a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reliability of the BES. The program shall include:			a Protection System maintenance program or a Protection System testing program for Protection Systems that affect the reliability of the BES.	Protection System maintenance program and a Protection System testing program for Protection Systems that affect the reliability of the BES.
PRC-005-1	R1.1.	Maintenance and testing intervals and their basis.	Maintenance and testing intervals and their basis was missing for no more than 25% of the applicable devices.	Maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the applicable devices.	Maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the applicable devices.	Maintenance and testing intervals and their basis was missing for more than 75% but of the applicable devices.
PRC-005-1	R1.2.	Summary of maintenance and testing procedures.	Summary of maintenance and testing procedures was missing for no more than 25% of the applicable devices.	Summary of maintenance and testing procedures was missing for more than 25% but less than or equal to 50% of the applicable devices.	Summary of maintenance and testing procedures was missing for more than 50% but less than or equal to 75% of the applicable devices.	Summary of maintenance and testing procedures was missing for more than 75% but of the applicable devices.
PRC-005-1	R2.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on	The responsible entity provided documentation of its Protection System maintenance and testing program for more than 30 but less than or equal to 40 days following a request from its Regional Reliability	The responsible entity provided documentation of its Protection System maintenance and testing program for more than 40 but less than or equal to 50 days following a request from its Regional Reliability	The responsible entity provided documentation of its Protection System maintenance and testing program for more than 50 but less than or equal to 60 days following a request from its Regional Reliability	The responsible entity did not provide documentation of its Protection System maintenance and testing program for more than 60 days following a request from its Regional Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		request (within 30 calendar days). The documentation of the program implementation shall include:	Organization and/or NERC.	Organization and/or NERC.	Organization and/or NERC.	Organization and/or NERC.
PRC-005-1	R2.1.	Evidence Protection System devices were maintained and tested within the defined intervals.	Evidence Protection System devices were maintained and tested within the defined intervals was missing for no more than 25% of the applicable devices.	Evidence Protection System devices were maintained and tested within the defined intervals was missing more than 25% but less than or equal to 50% of the applicable devices.	Evidence Protection System devices were maintained and tested within the defined intervals was missing more than 50% but less than or equal to 75% of the applicable devices.	Evidence Protection System devices were maintained and tested within the defined intervals was missing more than 75% of the applicable devices.
PRC-005-1	R2.2.	Date each Protection System device was last tested/maintained.	Date each Protection System device was last tested/maintained was missing no more than 25% of the applicable devices.	Date each Protection System device was last tested/maintained was missing for more than 25% but less than or equal to 50% of the applicable devices.	Date each Protection System device was last tested/maintained was missing for more than 50% but less than or equal to 75% of the applicable devices.	Date each Protection System device was last tested/maintained was missing for more than 75% of the applicable devices.
PRC-007-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall ensure that its UFLS program is consistent with its Regional Reliability Organization's UFLS program requirements.	The evaluation of the entity's UFLS program for consistency with its Regional Reliability Organization's UFLS program is incomplete or inconsistent in one or more of the Regional Reliability Organization program	The amount of load shedding is less than 95 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 90 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 85 percent of the Regional requirement in any of the load steps.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			requirements, but is consistent with the required amount of load shedding.			
PRC-007-0	R2.	The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database.	The responsible entity has demonstrated the reporting of information but failed to satisfy one database reporting requirements.	The responsible entity has demonstrated the reporting of information but failed to satisfy two database reporting requirements.	The responsible entity has demonstrated the reporting of information but failed to satisfy at three database reporting requirements.	The responsible entity has demonstrated the reporting of information but failed to satisfy four or more database reporting requirements or has not provided the information.
PRC-007-0	R3.	The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days).	The responsible entity has provided the documentation in more than 30 calendar days but less than 40 calendar days.	The responsible entity has provided the documentation in more than 39 calendar days but less than 50 calendar days.	The responsible entity has provided the documentation in more than 49 calendar days but less than 60 calendar days.	The responsible entity has not provided the documentation within 60 calendar days.
PRC-008-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification,	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment	The UFLS equipment identification, schedule for UFLS equipment testing or the schedule for UFLS equipment testing in the responsible entity's UFLS equipment

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.	maintenance and testing program was missing for no more than 25% of the applicable relays.	maintenance and testing program was missing for more than 25% but less than or equal to 50% of the applicable relays.	maintenance and testing program was missing for more than 50% but less than or equal to 75% of the applicable relays.	maintenance and testing program was missing for more than 75% of the applicable relays.
PRC-008-0	R2.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UFLS equipment maintenance and testing program for more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UFLS equipment maintenance and testing program for more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UFLS equipment maintenance and testing program for more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its UFLS equipment maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-009-0	R1.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions	The responsible entity that owns or operates a UFLS program failed to include one of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events	The responsible entity that owns or operates a UFLS program failed to include two of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events	The responsible entity that owns or operates a UFLS program failed to include three of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events	The responsible entity that owns or operates a UFLS program failed to conduct an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:	resulting in system frequency excursions below the initializing set points of the UFLS program.	resulting in system frequency excursions below the initializing set points of the UFLS program.	resulting in system frequency excursions below the initializing set points of the UFLS program.	points of the UFLS program.
PRC-009-0	R1.1.	A description of the event including initiating conditions.	N/A	N/A	N/A	The responsible entity failed to include a description of the event, including initiating conditions, that triggered an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.2.	A review of the UFLS set points and tripping times.	N/A	N/A	N/A	The responsible entity failed to include a review of the UFLS set points and tripping times in the analysis of the performance of UFLS equipment and Program

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.3.	A simulation of the event.	N/A	N/A	N/A	The responsible entity failed to conduct a simulation of the event that triggered an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.4.	A summary of the findings.	N/A	N/A	N/A	The responsible entity failed to include a summary of the findings in the analysis of the performance of UFLS equipment

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R2.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.	The responsible entity has provided the documentation in more than 90 calendar days but less than 105 calendar days.	The responsible entity has provided the documentation in more than 105 calendar days but less than 129 calendar days.	The responsible entity has provided the documentation in more than 129 calendar days but less than 145 calendar days.	The responsible entity has provided the documentation in 145 calendar days or more.
PRC-010-0	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	The responsible entity conducted an assessment of the effectiveness of its UVLS system within 5 years or as required by changes in system conditions but did not include the associated Transmission Planner(s) and Planning	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 5 years but did in less than or equal to 7 years.	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 7 years but did in less than or equal to 10 years.	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 10 years.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planning Authority(ies).	Authority(ies).			
PRC-010-0	R1.1.	This assessment shall include, but is not limited to:	N/A	The assessment of the effectiveness of the responsible entity's UVLS system did not address one of the elements in R1.1.1 through R1.1.3.	The assessment of the effectiveness of the responsible entity's UVLS system did not address two of the elements in R1.1.1 through R1.1.3.	The assessment of the effectiveness of the responsible entity's UVLS system did not address any of the elements in R1.1.1 through R1.1.3.
PRC-010-0	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.	The responsible entity is non-compliant in the coordination of the UVLS programs with no more than 25% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.	The responsible entity is non-compliant in the coordination of the UVLS programs with more than 25% but less than or equal to 50% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.	The responsible entity is non-compliant in the coordination of the UVLS programs with more than 50% but less than or equal to 75% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.	The responsible entity is non-compliant in the coordination of the UVLS programs with more than 75% of the appropriate protection and control systems in the Region and with other Regional Reliability Organizations.
PRC-010-0	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.	The responsible entity's analysis was non-compliant in that no more than 25% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-	The responsible entity's analysis was non-compliant in that more than 25% but less than or equal to 50% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-	The responsible entity's analysis was non-compliant in that more than 50% but less than or equal to 75% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-	The responsible entity's analysis was non-compliant in that more than 75% of the simulations needed to demonstrate consistency with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			0 were not performed.	003-0 and TPL-004-0 were not performed.	003-0 and TPL-004-0 were not performed.	0 were not performed.
PRC-010-0	R1.1.3.	A review of the voltage set points and timing.	The responsible entity's analysis is non-compliant in that a review of no more than 25% of the corresponding voltage set points and timing was not performed.	The responsible entity's analysis is non-compliant in that a review of more than 25% but less than or equal to 50% of the corresponding voltage set points and timing was not performed.	The responsible entity's analysis is non-compliant in that a review of more than 50% but less than 75% of the corresponding voltage set points and timing was not performed.	The responsible entity's analysis is non-compliant in that a review of more than 75% of the corresponding voltage set points and timing was not performed.
PRC-010-0	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).	The responsible entity provided documentation of its current UVLS program assessment more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its current UVLS program assessment for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-011-0	R1.	The Transmission Owner and Distribution Provider that owns a UVLS system shall have a UVLS equipment maintenance and testing program in place. This program shall include:	The responsible entity's UVLS equipment maintenance and testing program did not address one of the elements in R1.1 through R1.6.	The responsible entity's UVLS equipment maintenance and testing program did not address two or three of the elements in R1.1 through R1.6.	The responsible entity's UVLS equipment maintenance and testing program did not address four or five of the elements in R1.1 through R1.6.	The responsible entity's UVLS equipment maintenance and testing program did not address any of the elements in R1.1 through R1.6.
PRC-011-0	R1.1.	The UVLS system identification	The responsible	The responsible	The responsible	The responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		which shall include but is not limited to:	entity's UVLS program system identification did not address one of the elements in R1.1.1 through R1.1.4.	entity's UVLS program system identification did not address two of the elements in R1.1.1 through R1.1.4.	entity's UVLS program system identification did not address three of the elements in R1.1.1 through R1.1.4.	entity's UVLS program system identification did not address any of the elements in R1.1.1 through R1.1.4.
PRC-011-0	R1.1.1.	Relays.	The responsible entity's UVLS program system identification was missing no more than 25% of the applicable relays.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable relays.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable relays.	The responsible entity's UVLS program system identification was missing more than 75% of the applicable relays.
PRC-011-0	R1.1.2.	Instrument transformers.	The responsible entity's UVLS program system identification was missing no more than 25% of the applicable instrument transformers.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable instrument transformers.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable instrument transformers.	The responsible entity's UVLS program system identification was missing more than 75% of the applicable instrument transformers.
PRC-011-0	R1.1.3.	Communications systems, where appropriate.	The responsible entity's UVLS program system identification was missing no more than 25% of the appropriate communication systems.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the appropriate communication systems.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the appropriate communication systems.	The responsible entity's UVLS program system identification was missing more than 75% of the appropriate communication systems.
PRC-011-0	R1.1.4.	Batteries.	The responsible	The responsible	The responsible	The responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			entity's UVLS program system identification was missing no more than 25% of the applicable batteries.	entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable batteries.	entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable batteries.	entity's UVLS program system identification was missing more than 75% of the applicable batteries.
PRC-011-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the UVLS equipment.
PRC-011-0	R1.3.	Summary of testing procedure.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 75% of the UVLS equipment.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-011-0	R1.4.	Schedule for system testing.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 75% of the UVLS equipment.
PRC-011-0	R1.5.	Schedule for system maintenance.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for no more than 25% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 25% but less than or equal to 50% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 50% but less than or equal to 75% of the UVLS equipment.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 75% of the UVLS equipment.
PRC-011-0	R1.6.	Date last tested/maintained.	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for no more than 25% of	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 25% but	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 50% but	The responsible entity's UVLS equipment maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 75% of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the UVLS equipment.	less than or equal to 50% of the UVLS equipment.	less than or equal to 75% of the UVLS equipment.	the UVLS equipment.
PRC-011-0	R2.	The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its UVLS equipment maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-015-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall maintain a list of and provide data for existing and proposed SPSs as specified in Reliability Standard PRC-013-0_R 1.	N/A	The responsible entity's list of existing or proposed SPSs did not address one of the elements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.	The responsible entity's list of existing or proposed SPSs did not address two of the elements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.	The responsible entity's list of existing or proposed SPSs did not address any of the elements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.
PRC-015-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have evidence it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures as defined in Reliability Standard PRC-012-0_R1 prior to being	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		placed in service.	procedures did not address one of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	procedures did not address two to four of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	procedures did not address five to seven of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	procedures did not address eight or more of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.
PRC-015-0	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS data and the results of the studies that show compliance of new or functionally modified SPSs for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-016-0.1	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall analyze its SPS operations and maintain a record of all misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R 1.	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS	The responsible entity was not compliant in that evidence that it analyzed its SPS operations and maintained a record of all misoperations in accordance with the Regional SPS

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			review procedure did not address one of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.	review procedure did not address two to four of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.	review procedure did not address five to seven of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.	review procedure did not address eight or more of the elements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1.
PRC-016-0.1	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall take corrective actions to avoid future misoperations.	The responsible entity did not take corrective actions to avoid future SPS misoperations for no more than 25% of the events.	The responsible entity did not take corrective actions to avoid future SPS misoperations for more than 25% but less than or equal to 50% of the events.	The responsible entity did not take corrective actions to avoid future SPS misoperations for more than 50% but less than or equal to 75% of the events.	The responsible entity did not take corrective actions to avoid future SPS misoperations for more than 75% of the events.
PRC-016-0.1	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 90 but less than or equal to 120 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 120 but less than or equal to 150 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 150 but less than or equal to 180 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS misoperation analyses and the corrective action plans more than 180 days following a request from its Regional Reliability Organization and/or NERC.
PRC-017-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have a system maintenance and testing program(s) in place. The	The responsible entity's SPS system maintenance and testing program did not address one of the elements in R1.1	The responsible entity's SPS system maintenance and testing program did not address two or three of the	The responsible entity's SPS system maintenance and testing program did not address four or five of the elements	The responsible entity's SPS system maintenance and testing program did not address any of the elements in R1.1

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		program(s) shall include:	through R1.6.	elements in R1.1 through R1.6.	in R1.1 through R1.6.	through R1.6.
PRC-017-0	R1.1.	SPS identification shall include but is not limited to:	The responsible entity's SPS program identification did not address one of the elements in R1.1.1 through R1.1.4.	The responsible entity's SPS program identification did not address two of the elements in R1.1.1 through R1.1.4.	The responsible entity's SPS program identification did not address three of the elements in R1.1.1 through R1.1.4.	The responsible entity's SPS program identification did not address any of the elements in R1.1.1 through R1.1.4.
PRC-017-0	R1.1.1.	Relays.	The responsible entity's SPS program identification was missing no more than 25% of the applicable relays.	The responsible entity's SPS program identification was missing more than 25% but less than or equal to 50% of the applicable relays.	The responsible entity's SPS program identification was missing more than 50% but less than or equal to 75% of the applicable relays.	The responsible entity's SPS program identification was missing more than 75% of the applicable relays.
PRC-017-0	R1.1.2.	Instrument transformers.	The responsible entity's SPS program identification was missing no more than 25% of the applicable instrument transformers.	The responsible entity's SPS program identification was missing more than 25% but less than or equal to 50% of the applicable instrument transformers.	The responsible entity's SPS program identification was missing more than 50% but less than or equal to 75% of the applicable instrument transformers.	The responsible entity's SPS program identification was missing more than 75% of the applicable instrument transformers.
PRC-017-0	R1.1.3.	Communications systems, where appropriate.	The responsible entity's SPS program identification was missing no more than 25% of the appropriate communication	The responsible entity's SPS program identification was missing more than 25% but less than or equal to 50% of the appropriate	The responsible entity's SPS program identification was missing more than 50% but less than or equal to 75% of the appropriate	The responsible entity's SPS program identification was missing more than 75% of the appropriate communication

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			systems.	communication systems.	communication systems.	systems.
PRC-017-0	R1.1.4.	Batteries.	The responsible entity's SPS program identification was missing no more than 25% of the applicable batteries.	The responsible entity's UVLS program system identification was missing more than 25% but less than or equal to 50% of the applicable batteries.	The responsible entity's UVLS program system identification was missing more than 50% but less than or equal to 75% of the applicable batteries.	The responsible entity's UVLS program system identification was missing more than 75% of the applicable batteries.
PRC-017-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the SPS equipment.
PRC-017-0	R1.3.	Summary of testing procedure.	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 25% but less than or equal to 50% of the SPS	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 50% but less than or equal to 75% of the SPS	The responsible entity's SPS maintenance and testing program was non-compliant in that a summary of the testing procedure was missing for more than 75% of the SPS equipment.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				equipment.	equipment.	
PRC-017-0	R1.4.	Schedule for system testing.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system testing was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS equipment maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 25% but less than or equal to 50% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 50% but less than or equal to 75% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system testing was missing for more than 75% of the SPS equipment.
PRC-017-0	R1.5.	Schedule for system maintenance.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 25% but less than or equal to 50% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 50% but less than or equal to 75% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that a schedule for system maintenance was missing for more than 75% of the SPS equipment.
PRC-017-0	R1.6.	Date last tested/maintained.	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for no more than 25% of the SPS equipment.	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 25% but less than or equal to	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 50% but less than or equal to	The responsible entity's SPS maintenance and testing program was non-compliant in that the date last tested/maintained was missing for more than 75% of the SPS equipment.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				50% of the SPS equipment.	75% of the SPS equipment.	
PRC-017-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its SPS maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its SPS maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-018-1	R1.	Each Transmission Owner and Generator Owner required to install DMEs by its Regional Reliability Organization (reliability standard PRC-002 Requirements 1-3) shall have DMEs installed that meet the following requirements:	N/A	N/A	The responsible entity is not compliant in that the installation of DMEs does not include one of the elements in R1.1 and R1.2.	The responsible entity is not compliant in that the installation of DMEs does not include any of the elements in R1.1 and R1.2.
PRC-018-1	R1.1.	Internal Clocks in DME devices shall be synchronized to within 2 milliseconds or less of Universal Coordinated Time scale (UTC)	Less than or equal to 25% of DME devices did not comply with R1.1	Less than or equal to 37.5% but greater than 25% of DME devices did not comply with R1.1	Less than or equal to 50% but greater than 37.5% of DME devices did not comply with R1.1	Greater than 50% of DME devices did not did not comply with R1.1
PRC-018-1	R1.2.	Recorded data from each Disturbance shall be retrievable for ten calendar days.	Less than or equal to 12% of installed DME devices did not comply with R1.2	Less than or equal to 18% but greater than 12% of installed DME devices did not comply with R1.2	Less than or equal to 24% but greater than 18% of installed DME devices did not comply with R1.2	Greater than 24% of installed DME devices did not did not comply with R1.2
PRC-018-1	R2.	The Transmission Owner and Generator Owner shall each	The responsible entity is non-	The responsible entity is non-	The responsible entity is non-	The responsible entity is non-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		install DMEs in accordance with its Regional Reliability Organization's installation requirements (reliability standard PRC-002 Requirements 1 through 3).	compliant in that no more than 10% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.	compliant in that more than 10% but less than or equal to 20% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.	compliant in that more than 20% but less than or equal to 30% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.	compliant in that more than 30% of the DME devices were not installed in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 Requirements 1 through 3.
PRC-018-1	R3.	The Transmission Owner and Generator Owner shall each maintain, and report to its Regional Reliability Organization on request, the following data on the DMEs installed to meet that region's installation requirements (reliability standard PRC-002 Requirements1.1, 2.1 and 3.1):	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for one of the elements in Requirements 3.1 through 3.8.	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for two or three of the elements in Requirements 3.1 through 3.8.	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for four or five of the elements in Requirements 3.1 through 3.8.	The responsible entity was not compliant in that evidence that it maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for more than five of the elements in Requirements 3.1 through 3.8.
PRC-018-1	R3.1.	Type of DME (sequence of event recorder, fault recorder, or dynamic disturbance recorder).	Less than or equal to 25% of the required data per R3.1 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.1 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.1 was not maintained or reported.	Greater than 50% of the required data per R3.1 was not maintained or reported.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-018-1	R3.2.	Make and model of equipment.	Less than or equal to 25% of the required data per R3.2 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.2 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.2 was not maintained or reported.	Greater than 50% of the required data per R3.2 was not maintained or reported.
PRC-018-1	R3.3.	Installation location.	Less than or equal to 25% of the required data per R3.3 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.3 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.3 was not maintained or reported.	Greater than 50% of the required data per R3.3 was not maintained or reported.
PRC-018-1	R3.4.	Operational status.	Less than or equal to 25% of the required data per R3.4 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.4 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.4 was not maintained or reported.	Greater than 50% of the required data per R3.4 was not maintained or reported.
PRC-018-1	R3.5.	Date last tested.	Less than or equal to 25% of the required data per R3.5 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.5 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.5 was not maintained or reported.	Greater than 50% of the required data per R3.5 was not maintained or reported.
PRC-018-1	R3.6.	Monitored elements, such as transmission circuit, bus section, etc.	Less than or equal to 25% of the required data per R3.6 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.6 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.6 was not maintained or reported.	Greater than 50% of the required data per R3.6 was not maintained or reported.
PRC-018-1	R3.7.	Monitored devices, such as circuit	Less than or equal	Less than or equal	Less than or equal	Greater than 50% of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		breaker, disconnect status, alarms, etc.	to 25% of the required data per R3.7 was not maintained or reported.	to 37.5% but greater than 25% of the required data per R3.7 was not maintained or reported.	to 50% but greater than 37.5% of the required data per R3.7 was not maintained or reported.	the required data per R3.7 was not maintained or reported.
PRC-018-1	R3.8.	Monitored electrical quantities, such as voltage, current, etc.	Less than or equal to 25% of the required data per R3.8 was not maintained or reported.	Less than or equal to 37.5% but greater than 25% of the required data per R3.8 was not maintained or reported.	Less than or equal to 50% but greater than 37.5% of the required data per R3.8 was not maintained or reported.	Greater than 50% of the required data per R3.8 was not maintained or reported.
PRC-018-1	R4.	The Transmission Owner and Generator Owner shall each provide Disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements (reliability standard PRC-002 Requirement 4).	The responsible entity is not compliant in that it did not provide less than or equal to 10% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity is not compliant in that it did not provide less than or equal to 20% but greater than 10% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity is not compliant in that it did not provide less than or equal to 30% but greater than 20% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity is not compliant in that it did not provide greater than 30% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.
PRC-018-1	R5.	The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.	The responsible entity is not compliant in that no more than 25% of the data recorded by DMEs for Regional Reliability Organization-identified events	The responsible entity is not compliant in that more than 25% but less than or equal to 50% of the data recorded by DMEs for Regional Reliability	The responsible entity is not compliant in that more than 50% but less than or equal to 75% of the data recorded by DMEs for Regional Reliability	The responsible entity is not compliant in that more than 75% of the data recorded by DMEs for Regional Reliability Organization-identified events

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			was not archived for at least three years.	Organization-identified events was not archived for at least three years.	Organization-identified events was not archived for at least three years.	was not archived for at least three years.
PRC-018-1	R6.	Each Transmission Owner and Generator Owner that is required by its Regional Reliability Organization to have DMEs shall have a maintenance and testing program for those DMEs that includes:	N/A	N/A	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include one of the elements in R6.1 and 6.2.	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include any of the elements in R6.1 and 6.2.
PRC-018-1	R6.1.	Maintenance and testing intervals and their basis.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the DME equipment.
PRC-018-1	R6.2.	Summary of maintenance and testing procedures.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			missing for no more than 25% of the DME equipment.	missing for more than 25% but less than or equal to 50% of the DME equipment.	missing for more than 50% but less than or equal to 75% of the DME equipment.	missing for more than 75% of the DME equipment.
PRC-021-1	R1.	Each Transmission Owner and Distribution Provider that owns a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall annually update its UVLS data to support the Regional UVLS program database. The following data shall be provided to the Regional Reliability Organization for each installed UVLS system:	UVLS data was provided but did not address one of the elements in R1.1 through R1.5.	UVLS data was provided but did not address two of the elements in R1.1 through R1.5.	UVLS data was provided but did not address three of the elements in R1.1 through R1.5.	No annual UVLS data was provided OR UVLS data was provided but did not address four or more of the elements in R1.1 through R1.5.
PRC-021-1	R1.1.	Size and location of customer load, or percent of connected load, to be interrupted.	The responsible entity is non-compliant in the reporting of no more than 25% of the size or location of customer load, or percent of customer load to be interrupted.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the size or location of customer load, or percent of customer load to be interrupted.	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the size or location of customer load, or percent of customer load to be interrupted.	The responsible entity is non-compliant in the reporting of more than 75% of the size or location of customer load, or percent of customer load to be interrupted.
PRC-021-1	R1.2.	Corresponding voltage set points and overall scheme clearing times.	The responsible entity is non-compliant in the reporting of no more than 25% of the corresponding voltage set points and overall scheme clearing times.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the corresponding voltage set points	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the corresponding voltage set points	The responsible entity is non-compliant in the reporting of more than 75% of the corresponding voltage set points and overall scheme clearing times.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				and overall scheme clearing times.	and overall scheme clearing times.	
PRC-021-1	R1.3.	Time delay from initiation to trip signal.	The responsible entity is non-compliant in the reporting of no more than 25% of the time delay from initiation to trip signal data.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the time delay from initiation to trip signal data.	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the time delay from initiation to trip signal data.	The responsible entity is non-compliant in the reporting of more than 75% of the time delay from initiation to trip signal data.
PRC-021-1	R1.4.	Breaker operating times.	The responsible entity is non-compliant in the reporting of no more than 25% of the breaker operating times.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of the breaker operating times.	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of the breaker operating times.	The responsible entity is non-compliant in the reporting of more than 75% of the breaker operating times.
PRC-021-1	R1.5.	Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	The responsible entity is non-compliant in the reporting of no more than 25% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	The responsible entity is non-compliant in the reporting of more than 25% but less than or equal to 50% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection	The responsible entity is non-compliant in the reporting of more than 50% but less than or equal to 75% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection	The responsible entity is non-compliant in the reporting of more than 75% of any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Systems.	Systems.	
PRC-021-1	R2.	Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.	The responsible entity updated its UVLS data more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization.	The responsible entity did not update its UVLS data for more than 60 days following a request from its Regional Reliability Organization.
PRC-022-1	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:	The responsible entity failed to analyze and document no more than 25% of all UVLS operations and misoperations.	The responsible entity failed to analyze and document more than 25% but less than or equal to 50% of all UVLS operations and misoperations or the overall analysis program did not address one of the elements in R1.1 through R1.5.	The responsible entity failed to analyze and document more than 50% but less than or equal to 75% of all UVLS operations and misoperations or the overall analysis program did not address two or three of the elements in R1.1 through R1.5.	The responsible entity failed to analyze and document more than 75% of all UVLS operations and misoperations or the overall analysis program did not address four or more of the elements in R1.1 through R1.5.
PRC-022-1	R1.1.	A description of the event including initiating conditions.	The responsible entity's analysis is missing a description of the event including initiating conditions for no more than 25% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a description of the event including initiating conditions for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a description of the event including initiating conditions for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a description of the event including initiating conditions for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R1.2.	A review of the UVLS set points	The responsible	The responsible	The responsible	The responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and tripping times.	entity's analysis is missing a review of the UVLS set points and tripping times for no more than 25% of all UVLS operations and misoperations.	entity's analysis is missing a review of the UVLS set points and tripping times for more than 25% but less than 50% of all UVLS operations and misoperations.	entity's analysis is missing a review of the UVLS set points and tripping times for more than 50% but less than 75% of all UVLS operations and misoperations.	entity's analysis is missing a review of the UVLS set points and tripping times for more than 75% of all UVLS operations and misoperations.
PRC-022-1	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.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for no more than 25% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a simulation of the event, if deemed appropriate by the Regional Reliability Organization for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R1.4.	A summary of the findings.	The responsible entity's analysis is missing a summary of the findings for no more than 25% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a summary of the findings for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a summary of the findings for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	The responsible entity's analysis is missing a summary of the findings for more than 75% of all UVLS operations and misoperations.
PRC-022-1	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a	The responsible entity's analysis is missing a Corrective Action Plan to avoid future Misoperations of a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			similar nature for no more than 25% of all UVLS operations and misoperations.	similar nature for more than 25% but less than or equal to 50% of all UVLS operations and misoperations.	similar nature for more than 50% but less than or equal to 75% of all UVLS operations and misoperations.	similar nature for more than 75% of all UVLS operations and misoperations.
PRC-022-1	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.	The responsible entity provided documentation of the analysis of UVLS program performance more than 90 but less than or equal to 120 days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 120 but less than or equal to 150 days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 150 but less than or equal to 180 days following a request from its Regional Reliability Organization.	The responsible entity did not provide documentation of the analysis of UVLS program performance for more than 180 days following a request from its Regional Reliability Organization.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-001-1	R1.	Each Transmission Operator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area and shall exercise specific authority to alleviate operating emergencies.	N/A	N/A	N/A	The Transmission Operator has no evidence that clear decision-making authority exists to assure reliability in its area or has failed to exercise this authority to alleviate operating emergencies.
TOP-001-1	R2.	Each Transmission Operator shall take immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.	N/A	N/A	N/A	The Transmission Operator failed to have evidence that it took immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.
TOP-001-1	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives	N/A	N/A	N/A	The responsible entity failed to comply with reliability directives issued by the Reliability Coordinator or the Transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.				Operator (when applicable), when said directives would not have resulted in actions that would violate safety, equipment, regulatory or statutory requirements, or under circumstances that said directives would have resulted in actions that would violate safety, equipment, regulatory or statutory requirements the responsible entity failed to inform the Reliability Coordinator or Transmission Operator (when applicable) of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator could implement alternate remedial actions.
TOP-001-1	R4.	Each Distribution Provider and Load-Serving Entity shall	N/A	N/A	N/A	The responsible entity failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions.				comply with all reliability directives issued by the Transmission Operator, including shedding firm load, when said directives would not have resulted in actions that would violate safety, equipment, regulatory or statutory requirements, or under circumstances when said directives would have violated safety, equipment, regulatory or statutory requirements, the responsible entity failed to immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator could implement alternate remedial actions.
TOP-001-1	R5.	Each Transmission Operator shall inform its Reliability Coordinator and any other potentially affected Transmission	N/A	N/A	N/A	The Transmission Operator failed to inform its Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators of real-time or anticipated emergency conditions, and take actions to avoid, when possible, or mitigate the emergency.				Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, or failed to take actions to avoid, when possible, or mitigate the emergency.
TOP-001-1	R6.	Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.	N/A	N/A	N/A	The responsible entity failed to render all available emergency assistance to others as requested, after the requesting entity had implemented its comparable emergency procedures, when said assistance would not have resulted in actions that would violate safety, equipment, or regulatory or statutory requirements.
TOP-001-1	R7.	Each Transmission Operator and Generator Operator shall not remove Bulk Electric System facilities from service if removing those facilities would	N/A	N/A	N/A	The responsible entity removed Bulk Electric System facilities from service under

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		burden neighboring systems unless:				conditions other than those listed in TOP-001-1 R7.1 through R7.3 and removal of said facilities burdened a neighboring system.
TOP-001-1	R7.1.	For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	The Generator Operator failed to notify and coordinate with the Transmission Operator, or the Transmission Operator failed to notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.
TOP-001-1	R7.2.	For a transmission facility, the Transmission Operator shall notify and coordinate with its Reliability Coordinator. The Transmission Operator shall notify other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	The Transmission Operator failed to notify and coordinate with its Reliability Coordinator, or failed to notify other affected Transmission Operators, and coordinate the impact of removing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the Bulk Electric System facility.
TOP-001-1	R7.3.	When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.	N/A	N/A	N/A	The Generator Operator failed to notify the Transmission Operator, or the Transmission Operator failed to notify its Reliability Coordinator and adjacent Transmission Operators during periods when time did not permit such notifications and coordination, or when immediate action was required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities.
TOP-001-1	R8.	During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency	N/A	N/A	N/A	The responsible entity failed to take immediate actions to restore the Real and Reactive Power Balance during a system emergency, or the responsible entity failed to request emergency

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.				assistance from the Reliability Coordinator during periods when it was unable to restore the Real and Reactive Power Balance, or during periods when corrective actions or emergency assistance was not adequate to mitigate the Real and Reactive Power Balance, the responsible entity failed to implement firm load shedding.
TOP-002-2	R1.	Each Balancing Authority and Transmission Operator shall maintain a set of current plans that are designed to evaluate options and set procedures for reliable operation through a reasonable future time period. In addition, each Balancing Authority and Transmission Operator shall be responsible for using available personnel and system equipment to implement these plans to ensure that interconnected system reliability will be maintained.	N/A	N/A	The responsible entity maintained a set of current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period, but failed utilize all available personnel and system equipment to implement these plans to ensure that interconnected system reliability	The responsible entity failed to maintain a set of current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					will be maintained.	
TOP-002-2	R2.	Each Balancing Authority and Transmission Operator shall ensure its operating personnel participate in the system planning and design study processes, so that these studies contain the operating personnel perspective and system operating personnel are aware of the planning purpose.	N/A	N/A	N/A	The responsible entity failed to ensure its operating personnel participated in the system planning and design study processes.
TOP-002-2	R3.	Each Load-Serving Entity and Generator Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider. Each Balancing Authority and Transmission Service Provider shall coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed to coordinate its seasonal operations with its Transmission Operator.	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed to coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.
TOP-002-2	R4.	Each Balancing Authority and Transmission Operator shall	N/A	The responsible entity failed to	N/A	The responsible entity failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator, so that normal Interconnection operation will proceed in an orderly and consistent manner.		coordinate (where confidentiality agreements allow) its seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator.		coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator.
TOP-002-2	R5.	Each Balancing Authority and Transmission Operator shall plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.	N/A	N/A	N/A	The responsible entity failed to plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.
TOP-002-2	R6.	Each Balancing Authority and Transmission Operator shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional, and local reliability requirements.	N/A	N/A	N/A	The responsible entity failed to plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						subregional, and local reliability requirements.
TOP-002-2	R7.	Each Balancing Authority shall plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.
TOP-002-2	R8.	Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.
TOP-002-2	R9.	Each Balancing Authority shall plan to meet Interchange Schedules and Ramps.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet Interchange Schedules and Ramps.
TOP-002-2	R10.	Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).	N/A	N/A	N/A	The responsible entity failed to plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-002-2	R11.	The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs. Neighboring Transmission Operators shall utilize identical SOLs for common facilities. The Transmission Operator shall update these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject confidentiality requirements), and to its Reliability Coordinator.	N/A	N/A	The Transmission Operator performed seasonal, next-day, and current-day Bulk Electric System studies, reflecting current system conditions, to determine SOLs, but failed to make the results of Bulk Electric System studies available to all of the Transmission Operators, Balancing Authorities (subject confidentiality requirements), or to its Reliability Coordinator.	The Transmission Operator failed to perform seasonal, next-day, or current-day Bulk Electric System studies, reflecting current system conditions, to determine SOLs.
TOP-002-2	R12.	The Transmission Service Provider shall include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available Transfer Capability calculation processes.	N/A	N/A	N/A	The Transmission Service Provider failed to include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Transfer Capability calculation processes.
TOP-002-2	R13.	At the request of the Balancing Authority or Transmission Operator, a Generator Operator shall perform generating real and reactive capability verification that shall include, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, and provide the results to the Balancing Authority or Transmission Operator operating personnel as requested.	N/A	N/A	N/A	The Generator Operator failed to perform generating real and reactive capability verification that included, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, or failed to provide the results of generating real and reactive verifications Balancing Authority or Transmission Operator operating personnel, when requested.
TOP-002-2	R14.	Generator Operators shall, without any intentional time delay, notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics including but not limited to:	N/A	N/A	N/A	The Generator Operator failed to notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics.
TOP-002-2	R14.1.	Changes in real output capabilities.	N/A	N/A	N/A	The Generator Operator failed to notify its Balancing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Authority or Transmission Operator of changes in real output capabilities.
TOP-002-2	R14.2.	Automatic Voltage Regulator status and mode setting. (Retired August 1, 2007)				
TOP-002-2	R15.	Generation Operators shall, at the request of the Balancing Authority or Transmission Operator, provide a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).	N/A	N/A	N/A	The Generation Operator failed to provide, at the request of the Balancing Authority or Transmission Operator, a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).
TOP-002-2	R16.	Subject to standards of conduct and confidentiality agreements, Transmission Operators shall, without any intentional time delay, notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics including but not limited to:	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2	R16.1.	Changes in transmission facility	N/A	N/A	N/A	The Transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		status.				Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility status, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2	R16.2.	Changes in transmission facility rating.	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility rating, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2	R17.	Balancing Authorities and Transmission Operators shall, without any intentional time delay, communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.	N/A	N/A	N/A	The responsible entity failed to communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-002-2	R18.	Neighboring Balancing Authorities, Transmission Operators, Generator Operators, Transmission Service Providers, and Load-Serving Entities shall use uniform line identifiers when referring to transmission facilities of an interconnected network.	N/A	N/A	N/A	The responsible entity failed to use uniform line identifiers when referring to transmission facilities of an interconnected network.
TOP-002-2	R19.	Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations.	N/A	N/A	N/A	The responsible entity failed to maintain accurate computer models utilized for analyzing and planning system operations.
TOP-003-0	R1.	Generator Operators and Transmission Operators shall provide planned outage information.				
TOP-003-0	R1.1.	Each Generator Operator shall provide outage information daily to its Transmission Operator for scheduled generator outages planned for the next day (any foreseen outage of a generator greater than 50 MW). The Transmission Operator shall establish the outage reporting requirements.	N/A	N/A	N/A	The Generator Operator failed to provide outage information, in accordance with its Transmission Operators established outage reporting requirements, to its Transmission Operator for scheduled generator outages planned for the next day (any

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						foreseen outage of a generator greater than 50 MW).
TOP-003-0	R1.2.	Each Transmission Operator shall provide outage information daily to its Reliability Coordinator, and to affected Balancing Authorities and Transmission Operators for scheduled generator and bulk transmission outages planned for the next day (any foreseen outage of a transmission line or transformer greater than 100 kV or generator greater than 50 MW) that may collectively cause or contribute to an SOL or IROL violation or a regional operating area limitation. The Reliability Coordinator shall establish the outage reporting requirements.	N/A	N/A	N/A	The Transmission Operator failed to provide outage information, in accordance with its Reliability Coordinators established outage reporting requirement, to its Reliability Coordinator, and to affected Balancing Authorities and Transmission Operators for scheduled generator and bulk transmission outages planned for the next day (any foreseen outage of a transmission line or transformer greater than 100 kV or generator greater than 50 MW) that may collectively cause or contribute to an SOL or IROL violation or a regional operating area limitation.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-003-0	R1.3.	Such information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	N/A	N/A	N/A	The responsible entity failed to provide the information by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.
TOP-003-0	R2.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators as required.	N/A	N/A	N/A	The responsible entity failed to plan or coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators when required.
TOP-003-0	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan	The responsible entity planned and coordinated	N/A	N/A	The responsible entity failed to plan and coordinate

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and coordinate scheduled outages of telemetering and control equipment and associated communication channels between the affected areas.	scheduled outages of telemetering and control equipment and associated communication channels with its Reliability Coordinator, but failed to coordinate with affected neighboring Transmission Operators, Balancing Authorities, and Generator Operators.			scheduled outages of telemetering and control equipment and associated communication channels between the affected areas.
TOP-003-0	R4.	Each Reliability Coordinator shall resolve any scheduling of potential reliability conflicts.	N/A	N/A	N/A	The Reliability Coordinator failed to resolve any scheduling of potential reliability conflicts.
TOP-004-1	R1.	Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).	N/A	N/A	The Transmission Operator operated within the Interconnection Reliability Operating Limits (IROLs), but failed to operate within the System Operating Limits (SOLs).	The Transmission Operator failed to operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).
TOP-004-1	R2.	Each Transmission Operator shall operate so that instability, uncontrolled separation, or	N/A	N/A	N/A	The Transmission Operator failed to operate so that

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cascading outages will not occur as a result of the most severe single contingency.				instability, uncontrolled separation, or cascading outages would not occur as a result of the most severe single contingency.
TOP-004-1	R3.	Each Transmission Operator shall, when practical, operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by Regional Reliability Organization policy.	N/A	N/A	N/A	The Transmission Operator failed to operate (when practical) to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by Regional Reliability Organization policy.
TOP-004-1	R4.	If a Transmission Operator enters an unknown operating state (i.e., any state for which valid operating limits have not been determined), it will be considered to be in an emergency and shall restore operations to respect proven reliable power system limits within 30 minutes.	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 30 minutes but less than or equal to 35	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 35 minutes but less than or equal to 40	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 40 minutes but less than or equal to 45	The Transmission Operator entering an unknown operating state (i.e., any state for which valid operating limits have not been determined), failed to restore operations to respect proven reliable power system limits for more than 45 minutes.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			minutes.	minutes.	minutes.	
TOP-004-1	R5.	Each Transmission Operator shall make every effort to remain connected to the Interconnection. If the Transmission Operator determines that by remaining interconnected, it is in imminent danger of violating an IROL or SOL, the Transmission Operator may take such actions, as it deems necessary, to protect its area.	N/A	N/A	N/A	The Transmission Operator does not have evidence that the actions taken to protect its area, resulting in its disconnection from the Interconnection, were necessary to prevent the danger of violating an IROL or SOL.
TOP-004-1	R6.	Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including:	The Transmission Operator developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, including the elements listed in TOP-004-1 R6.1 through R6.6, but failed to include other Transmission Operators in the development of said	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include one of the elements listed in TOP-004-1	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include two of the elements listed in TOP-004-1	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include three or more of the elements listed in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			policies and procedures.	R6.1 through R6.6.	R6.1 through R6.6.	TOP-004-1 R6.1 through R6.6.
TOP-004-1	R6.1.	Equipment ratings.	The Transmission Operator failed to include equipment ratings in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-004-1	R6.2.	Monitoring and controlling voltage levels and real and reactive power flows.	The Transmission Operator failed to include monitoring and controlling voltage levels and real and reactive power flows in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-004-1	R6.3.	Switching transmission elements.	The Transmission Operator failed to include switching	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			transmission elements in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.			
TOP-004-1	R6.4.	Planned outages of transmission elements.	The Transmission Operator failed to include planned outages of transmission elements in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-004-1	R6.5.	Development of IROLs and SOLs.	The Transmission Operator failed to include development of IROLs and SOLs in the development, maintenance, and implementation of formal policies and	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			procedures to provide for transmission reliability as described in TOP-004-1 R6.			
TOP-004-1	R6.6.	Responding to IROL and SOL violations.	The Transmission Operator failed to include responding to IROL and SOL violations in the development, maintenance, and implementation of formal policies and procedures to provide for transmission reliability as described in TOP-004-1 R6.	N/A	N/A	N/A
TOP-005-1.1	R1.	Each Transmission Operator and Balancing Authority shall provide its Reliability Coordinator with the operating data that the Reliability Coordinator requires to perform operational reliability assessments and to coordinate reliable operations within the Reliability Coordinator Area.	The responsible entity failed to provide all of the data requested by its Reliability Coordinator.	N/A	N/A	The responsible entity failed to provide all of the data requested by its Reliability Coordinator.
TOP-005-1.1	R1.1.	Each Reliability Coordinator shall identify the data requirements from the list in Attachment 1-TOP-005-0 "Electric System Reliability	N/A	N/A	N/A	The Reliability Coordinator failed to identify the data necessary to perform operational

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Data" and any additional operating information requirements relating to operation of the bulk power system within the Reliability Coordinator Area.				reliability assessments and to coordinate reliable operations within the Reliability Coordinator Area.
TOP-005-1.1	R2.	As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."	N/A	N/A	N/A	The ISN data recipient failed to sign the NERC Confidentiality Agreement for "Electric System Reliability Data".
TOP-005-1.1	R3.	Upon request, each Balancing Authority and Transmission Operator shall provide to other Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability, the operating data that are necessary to allow these Balancing Authorities and Transmission Operators to perform operational reliability assessments and to coordinate reliable operations. Balancing Authorities and Transmission Operators shall provide the types of data as listed in Attachment 1-TOP-005-0 "Electric System Reliability Data," unless otherwise agreed to by the Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability.	The responsible entity failed to provide any of the data requested by other Balancing Authorities or Transmission Operators.	N/A	N/A	The responsible entity failed to provide all of the data requested by its host Balancing Authority or Transmission Operator.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-005-1.1	R4.	Each Purchasing-Selling Entity shall provide information as requested by its Host Balancing Authorities and Transmission Operators to enable them to conduct operational reliability assessments and coordinate reliable operations.	The responsible entity failed to provide any of the data requested by other Balancing Authorities or Transmission Operators.	N/A	N/A	The responsible entity failed to provide all of the data requested by its host Balancing Authority or Transmission Operator.
TOP-006-1	R1.	Each Transmission Operator and Balancing Authority shall know the status of all generation and transmission resources available for use.	N/A	N/A	N/A	The responsible entity failed to know the status of all generation and transmission resources available for use, even though said information was reported by the Generator Operator, Transmission Operator, or Balancing Authority.
TOP-006-1	R1.1.	Each Generator Operator shall inform its Host Balancing Authority and the Transmission Operator of all generation resources available for use.	N/A	N/A	N/A	The Generator Operator failed to inform its Host Balancing Authority and the Transmission Operator of all generation resources available for use.
TOP-006-1	R1.2.	Each Transmission Operator and Balancing Authority shall inform the Reliability Coordinator and other affected Balancing Authorities and Transmission	N/A	N/A	N/A	The responsible entity failed to inform the Reliability Coordinator and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators of all generation and transmission resources available for use.				other affected Balancing Authorities and Transmission Operators of all generation and transmission resources available for use.
TOP-006-1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources.	N/A	The responsible entity monitors the applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, but is not aware of the status of rotating and static reactive resources.	The responsible entity fails to monitor all of the applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of all rotating and static reactive resources.	The responsible entity fails to monitor any of the applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources.
TOP-006-1	R3.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide appropriate technical information concerning protective relays to their operating personnel.	The responsible entity failed to provide any of the appropriate technical information concerning protective relays to their operating personnel.	N/A	N/A	The responsible entity failed to provide all of the appropriate technical information concerning protective relays to their operating personnel.
TOP-006-1	R4.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have information, including weather forecasts and past load patterns,	N/A	N/A	The responsible entity has either weather forecasts or past load patterns, available to predict	The responsible entity failed to have both weather forecasts and past load patterns,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		available to predict the system's near-term load pattern.			the system's near-term load pattern, but not both.	available to predict the system's near-term load pattern.
TOP-006-1	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions and to indicate, if appropriate, the need for corrective action.	N/A	N/A	The responsible entity used monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions, but does not have indication of the need for corrective action.	The responsible entity failed to use monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions.
TOP-006-1	R6.	Each Balancing Authority and Transmission Operator shall use sufficient metering of suitable range, accuracy and sampling rate (if applicable) to ensure accurate and timely monitoring of operating conditions under both normal and emergency situations.	N/A	N/A	N/A	The responsible entity failed to use sufficient metering of suitable range, accuracy and sampling rate (if applicable) to ensure accurate and timely monitoring of operating conditions under both normal and emergency situations.
TOP-006-1	R7.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor system frequency.	N/A	N/A	N/A	The responsible entity failed to monitor system frequency.
TOP-007-0	R1.	A Transmission Operator shall inform its Reliability Coordinator when an IROL or SOL has been exceeded and the actions being	N/A	N/A	The Transmission Operator informed its Reliability Coordinator when	The Transmission Operator failed to inform its Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		taken to return the system to within limits.			an IROL or SOL had been exceeded but failed to provide the actions being taken to return the system to within limits.	Coordinator when an IROL or SOL had been exceeded.
TOP-007-0	R2.	Following a Contingency or other event that results in an IROL violation, the Transmission Operator shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes.	Following a Contingency or other event that resulted in an IROL violation of a magnitude up to and including 5%, the Transmission Operator failed to return its transmission system to within IROL in less than or equal to 35 minutes.	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within IROL in accordance with the following: (a) an IROL with a magnitude up to and including 5% for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (b) an IROL with a magnitude greater than 5% but less than or equal to 10% for a period of time less than or equal to 40 minutes, or (c) an IROL with a magnitude greater	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within IROL in accordance with the following: (a) an IROL with a magnitude up to and including 5% for a period of time greater than 45 minutes, or (b) an IROL with a magnitude greater than 5% but less than or equal to 10% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude greater than 10% but less than or equal to 15%	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within IROL in accordance with the following: (a) an IROL with a magnitude greater than 10% but less than or equal to 15% for a period of time greater than 45 minutes, or (b) an IROL with a magnitude greater than 15% but less than or equal to 20% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude greater than 20% but less

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than 10% but less than or equal to 15% for a period of time less than or equal to 35 minutes.	for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (d) an IROL with a magnitude greater than 15% but less than or equal to 20% for a period of time less than or equal to 40 minutes, or (e) an IROL with a magnitude greater than 20% but less than or equal to 25% for a period of time less than or equal to 35 minutes.	than or equal to 25% for a period of time greater than 35 minutes, or (d) an IROL with a magnitude greater than 25% for a period of greater than 30 minutes.
TOP-007-0	R3.	A Transmission Operator shall take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to comply with Requirement R 2.	N/A	N/A	N/A	The Transmission Operator failed to take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to return the transmission system to IROL within 30 minutes.
TOP-007-0	R4.	The Reliability Coordinator shall evaluate actions taken to address an IROL or SOL violation and, if the actions taken are not	N/A	N/A	N/A	The Reliability Coordinator failed to evaluate actions taken to address an

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		appropriate or sufficient, direct actions required to return the system to within limits.				IROL or SOL violation and, if the actions taken were not appropriate or sufficient, direct actions required to return the system to within limits.
TOP-008-1	R1.	The Transmission Operator experiencing or contributing to an IROL or SOL violation shall take immediate steps to relieve the condition, which may include shedding firm load.	N/A	N/A	N/A	The Transmission Operator experiencing or contributing to an IROL or SOL violation failed to take immediate steps to relieve the condition, which may have included shedding firm load.
TOP-008-1	R2.	Each Transmission Operator shall operate to prevent the likelihood that a disturbance, action, or inaction will result in an IROL or SOL violation in its area or another area of the Interconnection. In instances where there is a difference in derived operating limits, the Transmission Operator shall always operate the Bulk Electric System to the most limiting parameter.	N/A	The Transmission Operator operated to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection but failed to operate the Bulk Electric System to the most limiting parameter in instances where there was a	The Transmission Operator operated to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area but failed to operate to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in another area of the Interconnection.	The Transmission Operator failed to operate to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				difference in derived operating limits.		
TOP-008-1	R3.	The Transmission Operator shall disconnect the affected facility if the overload on a transmission facility or abnormal voltage or reactive condition persists and equipment is endangered. In doing so, the Transmission Operator shall notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection prior to switching, if time permits, otherwise, immediately thereafter.	N/A	The Transmission Operator disconnected the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered but failed to notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection either prior to switching, if time permitted, otherwise, immediately thereafter.	N/A	The Transmission Operator failed to disconnect the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered.
TOP-008-1	R4.	The Transmission Operator shall have sufficient information and analysis tools to determine the cause(s) of SOL violations. This analysis shall be conducted in all operating timeframes. The Transmission Operator shall use the results of these analyses to immediately mitigate the SOL violation.	N/A	N/A	The Transmission Operator had sufficient information and analysis tools to determine the cause(s) of SOL violations and used the results of these analyses to	The Transmission Operator failed to have sufficient information and analysis tools to determine the cause(s) of SOL violations or failed to use the results of analyses to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					immediately mitigate the SOL violation(s), but failed to conduct these analyses in all operating timeframes.	immediately mitigate the SOL violation.

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-001-0.1	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I. To be considered valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-001-0.1	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-001-	R1.3.	Be supported by a current or	The responsible	The responsible entity	The responsible	The responsible entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
0.1		past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category A of Table 1 (no contingencies). The specific elements selected (from each of the following categories) shall be acceptable to the associated Regional Reliability Organization(s).	entity is non-compliant with 25% or less of the sub-components.	is non-compliant with more than 25% but less than 50% of the sub-components.	entity is non-compliant with 50% or more but less than 75% of the sub-components.	is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R1.3.1.	Cover critical system conditions and study years as deemed appropriate by the entity performing the study.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-001-0.1	R1.3.2.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system testing) AND most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-001-0.1	R1.3.3.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system simulation testing show marginal conditions that may require longer lead-time solutions.
TPL-001-0.1	R1.3.4.	Have established normal (pre-contingency) operating procedures in place.	N/A	N/A	N/A	No precontingency operating procedures are in place for existing facilities.
TPL-001-0.1	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-001-0.1	R1.3.6.	Be performed for selected demand levels over the range of forecast system demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						over a range of forecast system demands.
TPL-001-0.1	R1.3.7.	Demonstrate that system performance meets Table 1 for Category A (no contingencies).	N/A	N/A	N/A	No past or current study results exist showing pre-contingency system analysis.
TPL-001-0.1	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-001-0.1	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-001-0.1	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category A.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category A planning

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requirements.
TPL-001-0.1	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-001-0_R1, the Planning Authority and Transmission Planner shall each:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon.	N/A	N/A	N/A	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category A planning requirements.
TPL-001-0.1	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	A schedule for the responsible entity's corrective action plan does not exist.
TPL-001-0.1	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	Anticipated in-service dates, for the responsible entity's corrective action plan do not exist.
TPL-001-0.1	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	The responsible entity failed to consider necessary lead times to implement its corrective action plan.
TPL-001-0.1	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed	N/A	N/A	N/A	The responsible entity has failed to demonstrate the continuing need for previously identified

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implementation plans are not needed.				facility additions through subsequent annual assessments.
TPL-001-0.1	R3.	The Planning Authority and Transmission Planner shall each document the results of these reliability assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-002-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-002-0	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-002-0	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-002-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-002-0	R1.3.1.	Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce	N/A	The responsible entity provided evidence through current or past studies and/or system simulation testing that selected NERC Category B contingencies were evaluated, however, no rational was provided to indicate	N/A	The responsible entity did not provided evidence through current or past studies and/or system simulation testing to indicate that any NERC Category B contingencies were evaluated.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		less severe system results shall be available as supporting information.		why the remaining Category B contingencies for their system were not evaluated.		
TPL-002-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-002-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies (and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are no longer valid.
TPL-002-0	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						planning horizon) when past or current year near-term studies and/or system simulation testing show marginal conditions that may require longer lead-time solutions.
TPL-002-0	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-002-0	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system Demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-002-0	R1.3.7.	Demonstrate that system performance meets Category B contingencies.	N/A	N/A	N/A	No past or current study results exist showing Category B contingency system analysis.
TPL-002-0	R1.3.8.	Include existing and planned facilities.	The responsible entity’s transmission model used for past	The responsible entity’s transmission model used for past or	N/A	The responsible entity's transmission model used for past or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.		current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-002-0	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-002-0	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-002-0	R1.3.11.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-002-0	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-002-0	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category B of Table I.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category B planning requirements.
TPL-002-0	R1.5.	Consider all contingencies applicable to Category B.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to 25% or less of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient 75% or more of all applicable contingencies.
TPL-002-0	R2.	When System simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-002-0_R1, the Planning Authority and Transmission Planner shall	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		each:				
TPL-002-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category B planning requirements.
TPL-002-0	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	A schedule for the responsible entity's corrective action plan does not exist.
TPL-002-0	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	Anticipated in-service dates, for the responsible entity's corrective action plan does not exist. This would reflect effective dates for pre-contingency operating procedures or in-service dates for proposed system changes.
TPL-002-0	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	The responsible entity failed to consider necessary lead times to implement its corrective action plan.
TPL-002-0	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not	N/A	N/A	N/A	The responsible entity has failed to demonstrate the continuing need for previously identified facility additions

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		needed.				through sub-sequent annual assessments.
TPL-002-0	R3.	The Planning Authority and Transmission Planner shall each document the results of its Reliability Assessments and corrective plans and shall annually provide the results to its respective Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-003-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:				
TPL-003-0	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-003-0	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-003-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-003-0	R1.3.1.	Be performed and evaluated only for those Category C	N/A	The responsible entity provided evidence	N/A	The responsible entity did not provided

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.		through current or past studies that selected NERC Category C contingencies were evaluated, however, no rational was provided to indicate why the remaining Category C contingencies for their system were not evaluated.		evidence through current or past studies to indicate that any NERC Category C contingencies were evaluated.
TPL-003-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-003-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies (and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						no longer valid.
TPL-003-0	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system testing show marginal conditions that may require longer lead-time solutions.
TPL-003-0	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-003-0	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-003-0	R1.3.7.	Demonstrate that System	N/A	N/A	N/A	No past or current

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		performance meets Table 1 for Category C contingencies.				study results exists showing Category C contingency system analysis.
TPL-003-0	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-003-0	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet System performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-003-0	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-003-0	R1.3.11.	Include the effects of existing	N/A	N/A	The responsible	The responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and planned control devices.			entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.
TPL-003-0	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those Demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-003-0	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category C.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category C planning requirements.
TPL-003-0	R1.5.	Consider all contingencies applicable to Category C.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient with respect to 25% or less of all applicable contingencies.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category C contingencies applicable to their system, but was deficient 75% or more of all applicable contingencies.

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-003-0	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-003-0_R1, the Planning Authority and Transmission Planner shall each:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-003-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category C planning requirements.
TPL-003-0	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	A schedule for the responsible entity's corrective action plan does not exist.
TPL-003-0	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	Anticipated in-service dates, for the responsible entity's corrective action plan does not exist. This would reflect effective dates for pre-contingency operating procedures or in-service dates for proposed system changes.
TPL-003-0	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	The responsible entity failed to consider necessary lead times to implement its

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						corrective action plan.
TPL-003-0	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	N/A	N/A	N/A	The responsible entity has failed to demonstrate the continuing need for previously identified facility additions through sub-sequent annual assessments.
TPL-003-0	R3.	The Planning Authority and Transmission Planner shall each document the results of these Reliability Assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-004-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Table I. To be valid, the Planning Authority's and Transmission	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planner's assessment shall:				
TPL-004-0	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-004-0	R1.2.	Be conducted for near-term (years one through five).	N/A	N/A	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period.
TPL-004-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category D contingencies of Table I. The specific elements selected (from within each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-004-0	R1.3.1.	Be performed and evaluated only for those Category D contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting	N/A	The responsible entity provided evidence through current or past studies that selected NERC Category D contingencies were evaluated, however, no rational was provided to indicate why the remaining Category D contingencies for their	N/A	The responsible entity did not provided evidence through current or past studies to indicate that any NERC Category D contingencies were evaluated.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		information.		system were not evaluated.		
TPL-004-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-004-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	N/A	N/A	N/A	The responsible entity did not perform a near-term Category D study and/or system simulation test in the most recent annual period AND system changes (actual or proposed) indicate that past studies and/or system simulation testing are no longer valid
TPL-004-0	R1.3.4.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-004-0	R1.3.5.	Include existing and planned facilities.	The responsible entity’s transmission model used for past or current studies and/or system simulation testing	The responsible entity’s transmission model used for past or current studies and/or system simulation testing properly	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			properly reflects existing facilities, but is deficient in reflecting planned facilities.	reflects planned facilities, but is deficient in reflecting existing facilities.		reflecting existing AND planned facilities.
TPL-004-0	R1.3.6.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-004-0	R1.3.7.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-004-0	R1.3.8.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.
TPL-004-0	R1.3.9.	Include the planned (including maintenance) outage of any bulk electric equipment	N/A	N/A	N/A	The responsible entity's transmission model used for past or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.				current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-004-0	R1.4.	Consider all contingencies applicable to Category D.	The responsible entity has considered the NERC Category D contingencies, but was deficient with respect to 25% or less of all applicable contingencies	The responsible entity has considered the NERC Category D contingencies, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category D contingencies, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category D contingencies, but was deficient 75% or more of all applicable contingencies.
TPL-004-0	R2.	The Planning Authority and Transmission Planner shall each document the results of its reliability assessments and shall annually provide the results to its entities' respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments but did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments AND did not annually provided them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-001-1	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.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 5% or less of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting between 5-10% of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 10-15%, inclusive, of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting greater than 15% of their individual and neighboring areas voltage levels and Mvar flows.
VAR-001-1	R2.	Each Transmission Operator shall acquire sufficient reactive resources 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.	The Transmission Operator acquired 95% but less than 100% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 90% but less than 95% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 85% but less than 90% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired less than 85% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.
VAR-001-1	R3.	The Transmission Operator	N/A	N/A	N/A	The Transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.				Operator did not specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1. to all of the parties involved.
VAR-001-1	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.	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing one or more entities. The missing entities shall represent less than 25% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing two or more entities. The missing entities shall represent less than 50% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing three or more entities. The missing entities shall represent less than 75% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing four or more entities. The missing entities shall represent 75% or more of those eligible for the list.
VAR-001-1	R3.2.	For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.	The Transmission Operator failed to notify up to 25% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 25% up to 50% of the associated Generator Owners of each generator that are on this exemption list.	The Transmission Operator failed to notify 50% up to 75% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 75% up to 100% of the associated Generator Owner of each generator that are on this exemption list.
VAR-001-1	R4.	Each Transmission Operator shall specify a voltage or Reactive Power schedule at	N/A	N/A	The Transmission Operator provide Voltage or Reactive Power schedules	The Transmission Operator provide No evidence that voltage or Reactive Power

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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).			were for some but not all generating units as required in R4.	schedules were provided to Generator Operators as required in R4.
VAR-001-1	R5.	Each Purchasing-Selling Entity shall arrange for (self-provide or purchase) reactive resources to satisfy its reactive requirements identified by its Transmission Service Provider.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 5% or less of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting between 5-10% of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 10-15%, inclusive, of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting greater than 15% of its reactive requirements.
VAR-001-1	R6.	The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			requirement, affecting 5% or less of the required resources.	directed by the requirement, affecting between 5-10% of the required resources.	requirement, affecting 10-15%, inclusive, of the required resources.	15% or greater of required resources.
VAR-001-1	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.	N/A	N/A	N/A	The Transmission Operator has not provided evidence to show that directives were issued to the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule in accordance with R6.1.
VAR-001-1	R7.	The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 5% or less of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting between 5-10% of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 10-15%, inclusive, of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting greater than 15% of the required devices.
VAR-001-1	R8.	Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources	The applicable entity did operate or direct the operation of capacitive and	The applicable entity did operate or direct the operation of	The applicable entity did operate or direct the operation of capacitive and	The applicable entity did operate or direct the operation of capacitive and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		within its area – including reactive generation scheduling; transmission line and reactive resource switching; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.	inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 5% or less of the required resources.	capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting between 5-10% of the required resources.	inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 10-15%, inclusive, of the required resources.	inductive reactive resources or load shedding within its area, as directed by the requirement, affecting greater than 15% of the required resources.
VAR-001-1	R9.	Each Transmission Operator shall maintain reactive resources to support its voltage under first Contingency conditions.	The Transmission Operator maintains 95% or more of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 85% or more but less than 95% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 75% or more but less then 85% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains less than 75% of the reactive resources needed to support its voltage under first Contingency conditions.
VAR-001-1	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.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting 5% or less of the resources.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting between 5-10% of the resources.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting 10-15%, inclusive, of the resources.	The applicable entity did not disperse and/or locate the reactive resources, as directed in the requirement, affecting greater than 15% of the resources.
VAR-001-1	R10.	Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies	The applicable entity did not correct the IROL or SOL violations and/or	The applicable entity did not correct the IROL or SOL violations	The applicable entity did not correct the IROL or SOL violations and/or	The applicable entity did not correct the IROL or SOL violations and/or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.	complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 5% or less of the violations.	and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting between 5-10% of the violations.	complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 10-15%, inclusive, of the violations.	complete the required IROL or SOL violation reporting, as directed by the requirement, affecting greater than 15% of the violations.
VAR-001-1	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.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes and a timeframe for making these changes, but failed to provide technical justification for these changes.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes, but failed to provide a timeframe for making these changes and technical justification for these changes.	The Transmission Operator failed to provide documentation to the Generator Owner specifying required step-up transformer tap changes, a timeframe for making these changes, and technical justification for these changes.	N/A
VAR-001-1	R12.	The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.	N/A	N/A	N/A	The Transmission Operator has failed to direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.
VAR-002-	R1.	The Generator Operator	The Generator	The Generator	The Generator	The Generator

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
1.1a		shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator.	Operator failed to notify the Transmission Operator as identified in R1 for less than 25% of its generators.	Operator failed to notify the Transmission Operator as identified in R1 for 25% or more but less tan 50% of its generators.	Operator failed to notify the Transmission Operator as identified in R1 for 50% or more but less tan 75% of its generators.	Operator failed to notify the Transmission Operator as identified in R1 for 75% or more of its generators.
VAR-002-1.1a	R2.	Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings. [1] as directed by the Transmission Operator	The Generator Operator failed to maintain a voltage or reactive power schedule for less than 25% of its generators.	The Generator Operator failed to maintain a voltage or reactive power schedule for 25% or more but less tan 50% of its generators.	The Generator Operator failed to maintain a voltage or reactive power schedule for 50% or more but less tan 75% of its generators.	The Generator Operator failed to maintain a voltage or reactive power schedule for 75% or more of its generators.
VAR-002-1.1a	R2.1.	When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.	The Generator Operator failed to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for less than 25% of its generators.	The Generator Operator failed to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for 25% or more but less tan 50% of its generators.	The Generator Operator failed to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for 50% or more but less tan 75% of its generators.	The Generator Operator to use an alternate method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule for 75% or more of its generators.
VAR-002-1.1a	R2.2.	When directed to modify voltage, the Generator	The Generator Operator failed to	The Generator Operator failed to	The Generator Operator failed to	The Generator Operator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operator shall comply or provide an explanation of why the schedule cannot be met.	comply with required voltage modifications or provide an explanation of why the modifications could not be met less the 25% of the time.	comply with required voltage modifications or provide an explanation of why the modifications could not be met less than 50% of the time but more than or equal to 25% of the time.	comply with required voltage modifications or provide an explanation of why the modifications could not be met less than 75% of the time but more than or equal to 50% of the time.	comply with required voltage modifications or provide an explanation of why the modifications could not be met more than 75% of the time.
VAR-002-1.1a	R3.	Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:	The Generator Operator had one incident of failing to notify the Transmission Operator as identified in R3.	The Generator Operator had more than one but less than five incidents of failing to notify the Transmission as identified in R3.1 R3.2.	The Generator Operator had more than five but less than ten incidents of failing to notify the Transmission Operator as identified in R3.1 R3.2	The Generator Operator had ten or more incidents of failing to notify the Transmission Operator as identified in R3.1 R3.2.
VAR-002-1.1a	R3.1.	A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.	N/A	N/A	N/A	The Generator Operator failed to notify the Transmission Operator of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1a	R3.2.	A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.	N/A	N/A	N/A	The Generator Operator failed to notify the Transmission Operator of a status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.
VAR-002-1.1a	R4.	The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.	The Generator Owner had one (1) incident of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.	The Generator Owner had more than one (1) incident but less than five (5) incidents of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater	The Generator Owner had more than five (5) incidents but less than ten (10) incidents of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.	The Generator Owner had more than ten (10) incidents of failing to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than the generator terminal voltage.		
VAR-002-1.1a	R4.1.	For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for information, as described in R4.1.1 through R4.1.4, regarding generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R4.1.1.	Tap settings.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for tap settings on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1a	R4.1.2.	Available fixed tap ranges.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for available fixed tap ranges on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R4.1.3.	Impedance data.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission Planner within 30 calendar days of a request for impedance data on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R4.1.4.	The +/- voltage range with step-change in % for load-tap changing transformers.	N/A	N/A	N/A	The Generator Owner failed to notify its associated Transmission Operator and Transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Planner within 30 calendar days of a request for the +/- voltage range with tap change in percent (%) for load-tap changing transformers on generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage.
VAR-002-1.1a	R5.	After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had one (1) incident of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had more than one (1) incident but less than or equal to five (5) incidents of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had more than five (5) incident but less than or equal to ten (10) incidents of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.	The Generator Owner had more than ten (10) incidents of failing to change the step-up transformer tap settings in accordance with the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.
VAR-002-	R5.1.	If the Generator Operator	The Generator	The Generator	The Generator	The Generator

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
1.1a		can’t comply with the Transmission Operator’s specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.	Operator had one (1) incident of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.	Operator had more than one (1) incident but less than or equal to five (5) incidents of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.	Operator had more than five (5) incident but less than or equal to ten (10) incidents of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.	Operator had more than ten (10) incidents of failing to notify and provide technical justification to the Transmission Operator concerning non-compliance with Transmission Operator's specifications.