May 27, 2009

VIA ELECTRONIC FILING

Claudine Dutil-Berry, Secretary of the Board
National Energy Board
444 Seventh Avenue SW
Calgary, Alberta
T2P 0X8

Re: *North American Electric Reliability Corporation*

Dear Ms. Dutil-Berry:

The North American Electric Reliability Corporation ("NERC") hereby submits this filing seeking approval for proposed modifications to Critical Infrastructure Protection ("CIP") Reliability Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1 and CIP-009-1. The modified Reliability Standards are redesignated as CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, CIP-006-2, CIP-007-2, CIP-008-2 and CIP-009-2 and are contained in **Exhibit A** to this petition.

The modifications addressed by this filing are in direct response to the Federal Energy Regulatory Commission's ("FERC") directives in Order No. 706, issued on January 18, 2008.[1] In that Order, FERC approved the CIP Version 1 Reliability Standards and associated implementation plan but also directed NERC to develop modifications to CIP Reliability Standards CIP-002-1 through CIP-009-1 to address specific concerns identified by FERC. The magnitude of the directives dictated by Order

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

No. 706 resulted in a phased approach to addressing those directives. This filing represents the result of Phase 1 of the overall plan for revising the CIP Reliability Standards. Subsequent phases of the project for modifying the CIP Reliability Standards will address the remainder of FERC's directives provided in Order No. 706 that are not addressed in this filing.

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

NERC's petition consists of the following:

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

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

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins

Attorney for North American Electric Reliability Corporation

BEFORE THE
NATIONAL ENERGY BOARD

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

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

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

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

May 27, 2009

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby requests approval of eight Critical Infrastructure Protection ("CIP") Reliability Standards, CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, CIP-006-2, CIP-007-2, CIP-008-2 and CIP-009-2 (the "Version 2 CIP Reliability Standards," or "Version 2 Standards"). These Version 2 Standards contain modifications to CIP Reliability Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1 and CIP-009-1 (the "Version 1 CIP Reliability Standards," or "Version 1 Standards"), consistent with FERC directives in Order No. 706, issued on January 18, 2008.[1]

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

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

Exhibit A to this filing sets forth the proposed Version 2 CIP Reliability Standards. **Exhibit B** contains the complete development record for the proposed

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

Version 2 Standards. This record includes the Standard Authorization Request ("SAR"), the ballot pool, the final ballot results by registered ballot body members, stakeholder comments received during the development of these Reliability Standards, and an explanation of how those comments were considered in revising the CIP Reliability Standards. **Exhibit C** contains the roster identifying the members of the Cyber Security Standard Drafting Team that developed the proposed Version 2 Standards. **Exhibit D** contains a redline/strikeout version showing the changes made to the Version 1 CIP Reliability Standards to develop the Version 2 Standards. NERC filed these proposed Reliability Standards and associated implementation plans with FERC on May 22, 2009, and is filing these proposed Reliability Standards with the other applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

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

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

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

III. BACKGROUND

A. FERC Directives

On August 28, 2006, NERC submitted to FERC for approval Reliability Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1 and CIP-009-1.[3] These eight CIP Reliability Standards were approved in FERC's Order No. 706 along with NERC's implementation plan that set milestones for responsible entities to achieve full compliance with the CIP Reliability Standards.[4] In Order No. 706, FERC directed NERC to develop modifications to the CIP Reliability Standards through its reliability standards development process to address specific concerns identified by FERC.[5] The Version 2 CIP Reliability Standards presented in this filing represent NERC's Phase 1 efforts to comply with FERC's directives provided in Order No. 706. Subsequent phases of the project for modifying the CIP Reliability Standards will address the remainder of FERC's directives provided in Order No. 706 which are not addressed in this filing. Specifically, the following proposed changes included in Order No. 706 are addressed by this filing:

- removal of the term "reasonable business judgment" from the purpose section of each Reliability Standard;
- where applicable, removal of the phrase "acceptance of risk" from each Reliability Standard;
- revision to R4 in Reliability Standard CIP-002-2 to specify that the senior manager must annually approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets;

[3] *See North American Electric Reliability Council, et al.*, "Petition of the North American Electric Reliability Council and North American Electric Reliability Corporation for Approval of Proposed Reliability Standards," *Docket No. RM06-16-000* (August 28, 2006).
[4] Order No. 706 at PP 1 and 13.
[5] Order No. 706 at P 30. The Commission stated that "*any modification to a Reliability Standard, including a modification that addresses a Commission directive, must be developed and fully vetted through NERC's Reliability Standard development process.*"

- revision to the Applicability section of Reliability Standard CIP-003-2 to require that all Responsible Entities must comply with R2 of Reliability Standard CIP-003-2;

- revision to R2 of Reliability Standard CIP-003-2 to specify that a single manager with overall responsibility and authority be designated;

- revision to R2.3 in Reliability Standard CIP-003-2 to specify that delegations of authority must be documented;

- revision to R1 in Reliability Standard CIP-004-2 to clarify that the Responsible Entity shall establish, document, implement, and maintain, a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices;

- revision to R2 in Reliability Standard CIP-004-2 to specify that all employees with authorized access must be trained prior to access, except in specified circumstances such as an emergency;

- revision to R2 in Reliability Standard CIP-004-2 to clarify that the Responsible Entity shall establish, document, implement, and maintain, an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets;

- revision to R3 in Reliability Standard CIP-004-2 to clarify that the Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, prior to personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets;

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

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

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

- revision to the Implementation Plan for the Version 2 CIP Reliability Standards to clarify the formula to determine the "effective date" of the

standards for each stakeholder and to provide an example of the calculation; and

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

B. Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC *Reliability Standards Development Procedure*, which is incorporated into the NERC Rules of Procedure as Appendix 3A.[6] NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards.

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

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

C. Developmental History of the CIP Reliability Standards

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

The extensive scope of Project 2008-06 in responding to Order No. 706 led the Cyber Security SDT to develop a multiphase strategy to revise the CIP Reliability Standards and the associated implementation plan for these standards. The work reflected in this filing represents Phase 1 of that work plan. Phase 1 includes some of the necessary modifications to the CIP-002-1 through CIP-009-1 Reliability Standards directed by Order No. 706. Those modifications to the CIP Reliability Standards directed by FERC in Order No. 706 that are not included in this filing will be addressed in later phases of the work plan for Project 2008-06 Cyber Security Order No. 706 and will be filed with FERC and applicable governmental authorities in Canada at a later time.

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

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

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

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

IV. PROPOSED MODIFICATIONS TO CIP RELIABILITY STANDARDS

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

- Removal of Specific Terminology:[7]
  - From the Purpose Section: Removal of the term "reasonable business judgment."
  - Where applicable, removal of the phrase "acceptance of risk."

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

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

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

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

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

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

[7] Order No. 706 at P 14.

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

CIP-002-2 Critical Cyber Asset Identification

- As directed in Order No. 706:[8]
  - R4 Annual Approvals: Add that the senior manager shall annually review and approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets as required in prior version.

CIP-003-2 Security Management Controls

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

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

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

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

CIP-004-2 Personnel and Training

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

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

[8] Order No. 706 at P 294

except in specified circumstance such as an emergency. This replaces the allowance for 30 days to complete personnel risk assessment and adds a provision for emergency situations.

CIP-005-2 Electronic Security Perimeter(s)

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

CIP-006-2 Physical Security

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

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

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

- As directed in Order No. 706:

- R1.7 Updates to the Physical Security Plan: Shortens the time for updates to the Physical Security Plan to 30 calendar days rather than 90 days and adds the word "completion" to the requirement.
- R1 Physical Security Plan: Changes the term "a senior manager" to "the senior manager."

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

CIP-007-2 Systems Security Management

§ As directed in Order No. 706:
- R2.3 Ports and Services: Removal of the term "or an acceptance of risk."
- R3.2 Security Patch Mgt.: Removal of the term "or an acceptance of risk."
- R4.1 Malicious Software Prevention: Removal of the term "or an acceptance of risk."
- R9 Documentation Review and Maintenance: Shortens the time frame to update documentation in response to a system or control change from 90 to 30 calendar days and further clarifies this timeframe to begin after such change is complete.

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

CIP-008-2 Incident Reporting and Response Planning

§ As directed in Order No. 706:
- R1.4 Updating the Cyber Security Incident Response Plan: Shortens the timeframe to update the Incident Response Plan from 90 to 30 calendar days.

- R1.6 Testing of the Incident Response Plan: Adds language to clarify that testing need not require a responsible entity to remove any systems from service.

§ Clarifications to ensure that requirements must be implemented.

§ R1 Incident Response Plan: Explicitly requires implementation.

CIP-009-2 Recovery Plans for Critical Cyber Assets

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

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

§ When these standards become effective, the Responsible Entities identified in the Applicability section of the Standard must comply with the requirements. These include:

  - Reliability Coordinator
  - Balancing Authority
  - Interchange Authority
  - Transmission Service Provider
  - Transmission Owner
  - Transmission Operator
  - Generator Owner
  - Generator Operator
  - Load Serving Entity
  - NERC
  - Regional Entity

§ The Implementation Plan proposes an effective date for the Version 2 CIP Reliability Standards as the first day of the third calendar quarter (*i.e.*, a minimum of two full calendar quarters and not more than three calendar quarters) after approval. Additionally, the Implementation Plan provides that newly registered *entities* must comply with the requirements of the Version 2 CIP Reliability

Standards within 24 months of registration. The sole exception is CIP-003-2 Requirement R2, where the newly registered entity must comply within 12 months of registration.

§ Furthermore, NERC's Implementation Plan addresses newly *identified* Critical Cyber Assets based on whether or not the entity has an active CIP program. The plan provides an implementation schedule with "compliant" milestones for each CIP Reliability Standard. All timelines are specified as an offset from the date when the Critical Cyber Asset was newly identified.

1. Summary of Stakeholder Comments

The comments raised a variety of issues from minor text edits to compliance concerns, and the SDT prepared a written response to each set of comments received. Some of the more contentious comments centered around the appointment of one senior manager with authority to approve an entity's filing regarding these standards, as well as the latitude regarding the delegation of the senior manager's responsibilities to others. Concerns were also raised regarding the data retention requirements, the confidentiality of the data retained over extended periods of time, the acceptance of risk, and the removal of the "reasonable business judgment" language. The SDT identified and considered several arguments asserted by stakeholders during the initial ballot of the Version 2 CIP Reliability Standards both for and against approving the proposed CIP Reliability Standards, which are summarized below.

i. Designation of a Single Senior Manager

The designation of a single senior manager, as required by FERC in its discussion of Reliability Standard CIP-003-1 R2 in Order No. 706 was considered to be overly

prescriptive. Entities objected to this requirement by arguing that the standards would prescribe their corporate governance. To a lesser extent, some entities stated that they would prefer to see the senior manager requirement moved to Reliability Standard CIP-002-2.

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

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

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

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

In response to these concerns, the SDT stated that the term "continuous" does not change the original intent or the ability to audit the requirement. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. In response to concerns raised regarding how to demonstrate compliance, the SDT noted that there are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).[9]

iii. Technical Feasibility Exception ("TFE") Process

Entities commented that the TFE process, as the alternative to "Reasonable Business Judgment" language, should have been made available in the standard and not moved to the Uniform Compliance Monitoring and Evaluation Program ("CMEP") in the NERC Rules of Procedure. The concerns raised included the need to define the TFE process in the standards themselves, and the TFE stipulation that the standard must provide for feasibility or the TFE process will not allow the Entity to seek relief. Concerns were also raised with respect to the removal of the assertion in Section D 1.4.2 (Additional Compliance Information) of the NERC Rules of Procedure that duly authorized exceptions would not result in non-compliance.

In response to these concerns, the SDT provided that it has no authority over the approval process for changes to the NERC Rules of Procedure, noting the industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees and will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommended that the industry take

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

advantage of every opportunity to influence the TFE development process. The SDT also stated that an exception against the Responsible Entity's compliance policy does not relieve the Entity from compliance with a requirement of the standard, and therefore, the SDT asserted, a properly approved exception to the Responsible Entity's security policy will not result in non-compliance. Because the exception against a company policy is a separate issue from an exception against the requirement of the standard, a Responsible Entity may find it has to process both types of exceptions.

iv. Modification to Documentation Update Timeframe Requirements

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

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

A number of additional comments provided during the balloting process included concerns with requirements that were not revised in Phase 1 of the development of Version 2 of the CIP Reliability Standards. These comments were deferred by the SDT

with a recommendation to resubmit the comments in future SDT revisions to the CIP Reliability Standards, as appropriate.

V. JUSTIFICATION FOR APPROVAL OF PROPOSED CIP RELIABILITY STANDARDS

As FERC noted in Order No. 706, the CIP Reliability Standards, together, provide baseline requirements for the protection of critical cyber assets that support an important reliability goal for the bulk power system.[10] The CIP Reliability Standards provide a comprehensive set of requirements to protect the bulk power system from malicious cyber attacks by requiring bulk power system users, owners and operators to establish a risk-based vulnerability assessment methodology to identify and prioritize critical assets and critical cyber assets. The Version 2 CIP Reliability Standards proposed support these reliability goals and directly address concerns identified by FERC in Order No. 706.

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

[10] Order No. 706 at P 24.

requests approval of the Version 2 CIP Reliability Standards to help strengthen the security of the bulk power system.

VI. CONCLUSION

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

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

Respectfully submitted,

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

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

Exhibit A

Reliability Standards Proposed for Approval

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-2

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

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

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

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None.

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-2

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

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

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-2

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

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

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

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

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

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

2. Number: CIP-005-2

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

4. Applicability

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

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

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

R2.5.2. The authentication methods.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

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

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

A. Introduction

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

2. Number: CIP-006-2

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

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

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

R2.1. Be protected from unauthorized physical access.

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

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

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

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

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

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

1.5. Additional Compliance Information.

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

E. Regional Variances

None identified.

Version History

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

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

A. Introduction

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

2. Number: CIP-008-2

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

4. Applicability

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

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

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

C. Measures

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

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

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

E. Regional Variances

None identified.

Version History

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

A. Introduction

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

2. Number: CIP-009-2

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

4. Applicability:

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

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

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

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

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

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

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

B. Requirements

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

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

Exhibit B

Record of Development of Proposed Reliability Standards

(Provided Upon Request)

Exhibit C

The Cyber Security Standard Drafting Team Roster

Exhibit C
Cyber Security Order 706 Standard Drafting Team Roster (Project 2008-06)

Jeri Domingo Brewer — Chair Special Assistant	U.S. Bureau of Reclamation 2800 Cottage Way — MP-106 Sacramento, California 95825	(916) 978-5198 jbrewer@mp.usbr.gov
Kevin B. Perry — Vice Chair Director, Critical Infrastructure Protection	Southwest Power Pool Regional Entity 415 North McKinley — Suite 140 Little Rock, Arkansas 72205	(501) 614-3251 (501) 664-6923 Fx kperry@spp.org
Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@opg.com
Jackie Collett Cyber Security Operations Engineer	Manitoba Hydro 1565 Willson Place — P.O. Box 815 Winnipeg, Manitoba R3C 2P4	(204) 477-7709 jcollett@hydro.mb.ca
Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@southernco.com
Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@kcpl.com
Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets — 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@duke-energy.com
Scott W. Fixmer Senior Security Analyst Exelon Corporate Security	Exelon Corporation 1700 Spencer Road Joliet, Louisiana 60433	(815) 724-7203 (815) 724-7032 Fx Scott.Fixmer@exeloncorp.com
Gerald S. Freese Director, Enterprise Information Security	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
Philip Huff Security Analyst	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
Frank Kim Director, Power System Information Technology	Hydro One Networks, Inc. 49 Sarjeant Drive Barrie, Ontario L4N 4V9	(705) 792-3033 frank.kim@hydroone.com
Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
John Lim, CISSP Department Manager	Consolidated Edison Co. of New York 4 Irving Place — Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
David L. Norton Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue — MS: L-ENT-24A New Orleans, Louisiana 70113	(504) 576-5469 (504) 576-5123 Fx dnorto1@entergy.com

Christopher A. Peters Vice President, Cybersecurity Solutions	ICF International 9300 Lee Highway Fairfax, Virginia 22031	(703) 934-3864 cpeters@icfi.com
David S Revill Group Lead, Electronic Maintenance	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@gatrans.com
Scott Rosenberger Manager of Information Technology	Luminant Energy 500 North Akard Dallas, Texas 75201	(214) 875-8731 scott.rosenberger@luminant.com
Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
Jon Stanford Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@bpa.gov
Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive — Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 Fx keith.stouffer@nist.gov
John D. Varnell Technology Director	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 Fx jvarnell@tnsk.com
William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue — Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@aps.com
Hal Beardall — Consultant to NERC	Florida State University Morgan Building — Suite 236 2035 East Paul Dirac Drive — P.O. Box 3062777 Tallahassee, Florida 32310-4161	(850) 644-4945 (850) 644-4968 Fx hbeardall@fsu.edu
Joseph Bucciero President and Executive Consultant — **Consultant to NERC**	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525	(267) 981-5445 joe.bucciero@gmail.com
Robert M. Jones Director Florida Conflict Resolution Consortium — **Consultant to NERC**	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive Tallahassee, Florida 32310-4161	(850) 644-6320 (850) 644-4968 Fx rmjones@fsu.edu
Stuart Langton, PhD Senior Fellow — **Consultant to NERC**	Florida State University 2010 Wild Lime Drive Sanibel, Florida 33957	(239) 395-9694 (239) 395-3230 Fx slangton@mindspring.com
Tom Hofstetter NERC Regional Compliance Auditor	North American Electric Reliability Corporation Noblesville, Indiana 46062	609-651-2532 (609) 452-0550 Fx tom.hofstetter@nerc.net
Roger Lampila NERC Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx roger.lampila@nerc.net
Scott Mix NERC Manager of Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (801) 203-8204 Fx scott.mix@nerc.net

Julia Souder NERC Director of Inter-Governmental Relations	North American Electric Reliability Corporation 1120 G Street, N.W. — Suite 990 Washington, D.C. 20005-3801	(202) 393-3998 (202) 393-3955 Fx julia.souder@nerc.net
David Taylor NERC Manager of Standards Development	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx david.taylor@nerc.net
Todd Thompson NERC Compliance Investigator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx todd.thompson@nerc.net

Exhibit D

CIP Standards Redline/Strikeout Version
Proposed Changes to Standards

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~1~~2

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

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

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

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 ~~Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor~~None.

2. ~~Levels of Non-Compliance~~Violation Severity Levels (To be developed later.)

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

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

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

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

E. Regional ~~Differences~~Variances

None identified.

Version History

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

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~1~~2

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

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

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements~~ Responsible Entity shall make available documentation of ~~Standard CIP-003:~~

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

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

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

M4. ~~Documentation of the~~The Responsible ~~Entity's~~Entity shall make available documentation of its information protection program as specified in Requirement R4.

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

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

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

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

~~**2. Levels of Noncompliance**~~

~~**2.1. Level 1:**~~

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

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

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

~~**2.2. Level 2:**~~

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

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

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

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

~~2.3. Level 3:~~

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

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

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

~~2.4. Level 4:~~

~~2.4.1 No cyber security policy exists; or,~~

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

~~2.4.3 No documented change control and configuration management process exists.~~

1.5.1 None

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

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to	

		include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-1~~2~~

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

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

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

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

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

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

R2. Training — The Responsible Entity shall establish, document, implement, and maintain~~, and document~~ an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets~~, and review the~~. The cyber security training program shall be reviewed annually, at a minimum, and ~~update as~~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 ~~within ninety calendar days of~~prior to their being granted such ~~authorization.~~access except in specified circumstances such as an emergency.

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

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

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

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

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

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

C. Measures

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

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

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

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

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

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.4.3 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

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

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

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

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

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

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

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

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

~~2.2. Level 2:~~

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

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

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

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

~~2.3. Level 3:~~

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

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

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

~~2.4. Level 4:~~

~~2.4.1 No documented training program exists; or,~~

~~2.4.2 No documented personnel risk assessment program exists; or,~~

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

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

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to	

		clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to “Critical Cyber Assets”. Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

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

2. Number: CIP-005-1~~2~~

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

4. Applicability

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations.~~Entity

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

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

R2.5.2. The authentication methods.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

M4. ~~Documentation of the Responsible Entity's~~The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

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

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.4.3 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

~~**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior~~

manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

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

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

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

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

2.2. Level 2:

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

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

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

2.3. Level 3:

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

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

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

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

2.3.5 Electronic Access Monitoring:

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

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

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

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

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

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

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

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

E. Regional ~~Differences~~Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	

A. Introduction

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

2. Number: CIP-006-1~~1~~2

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

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

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

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

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

R1.1. ~~Processes to ensure and document that all~~ All Cyber Assets within an Electronic Security Perimeter ~~also~~ shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the

Responsible Entity shall deploy and document alternative measures to control physical access to ~~the Critical~~such Cyber Assets.

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

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

R1.4. ~~Procedures for the appropriate~~Appropriate use of physical access controls as described in Requirement ~~R3~~R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

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

R1.6. ~~Procedures for~~Continuous escorted access within the ~~physical security perimeter~~Physical Security Perimeter of personnel not authorized for unescorted access.

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

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

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

R2.1. Be protected from unauthorized physical access.

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

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

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

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

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

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

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

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3R4.

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

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3R4.

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

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3R4, R5, and R4R6 function properly. The program must include, at a minimum, the following:

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

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6R8.1.

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

C. Measures

The following measures will be used to demonstrate compliance withResponsible Entity shall make available the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

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

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

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement ~~R2~~R4.

M5. ~~Documentation~~The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement ~~R3~~R5.

M6. ~~Documentation~~The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement ~~R4~~R6.

M7. ~~Access~~The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement ~~R5~~R7.

M8. ~~Documentation~~The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement ~~R6.~~R8.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements ~~R5~~R7 and ~~R6~~R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

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

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

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

~~2.~~ Violation Severity Levels ~~of Noncompliance~~

~~**2.1. Level 1:**~~

2. ~~The physical security plan exists, but has not been updated within ninety calendar days of a modification to~~**(Under development by the** ~~plan or any of its components; or,~~**CIP VSL Drafting Team)**

~~**3.1.1** Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~**3.1.2** Required documentation exists but has not been updated within ninety calendar days of a modification.; or,~~

~~**3.1.3** Physical access logs are retained for a period shorter than ninety days; or,~~

~~**3.1.4** A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,~~

~~**3.1.5** One required document does not exist.~~

~~**3.2. Level 2:**~~

~~**3.2.1** The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,~~

~~**3.2.2** Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~**3.2.3** Required documentation exists but has not been updated within six calendar months of a modification; or~~

~~**3.2.4** More than one required document does not exist.~~

~~**3.3. Level 3:**~~

~~3.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,~~

~~3.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~3.3.3 No logs of monitored physical access are retained.~~

~~3.4. Level 4:~~

~~3.4.1 No physical security plan exists; or,~~

~~3.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,~~

~~3.4.3 No maintenance or testing program exists.~~

E. Regional ~~Differences~~Variances

None identified.

Version History

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

		Enforcement Authority.	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~1~~2

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

4. Applicability:

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

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

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):~~

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service

packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:~~

M1. ~~Documentation of the~~ Responsible ~~Entity's~~Entity shall make available documentation of its security test procedures as specified in Requirement R1.

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.4.3 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

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

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

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~**2.1.1** System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or~~

~~**2.1.2** One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,~~

~~**2.1.3** One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,~~

~~**2.1.4** Any one of:~~

- ~~Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,~~
- ~~A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,~~
- ~~Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.~~

~~2.2. Level 2:~~

~~2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.3. Level 3:~~

~~2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4. Level 4:~~

~~2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,~~

~~2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.~~

~~2.4.3 No logs exist.~~

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

E. Regional ~~Differences~~Variances

None identified.

Version History

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

A. Introduction

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

2. Number: CIP-008-1~~2~~

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

4. Applicability

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

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional ~~Reliability Organizations~~Entity.

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

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-008:~~

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

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

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

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

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

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

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

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

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of CIP-008:~~

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

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

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The ~~compliance monitor~~Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

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

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

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

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

~~2. Levels of Noncompliance~~

~~**2.1. Level 1:** A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.~~

~~**2.2. Level 2:**~~

~~**2.2.1** A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,~~

~~**2.2.2** A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,~~

~~**2.2.3** Records related to reportable Cyber Security Incidents were not retained for three calendar years.~~

~~**2.3. Level 3:**~~

~~**2.3.1** A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,~~

~~**2.3.2** A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.~~

~~**2.4. Level 4:** A Cyber Security Incident response plan does not exist.~~

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

E. Regional ~~Differences~~Variances

None identified.

Version History

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

A. Introduction

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

2. Number: CIP-009-1~~2~~

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

4. Applicability:

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

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional ~~Reliability Organizations~~Entity

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

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

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

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

5. Effective Date: ~~June 1, 2006~~ The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-009:~~

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

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

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

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

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

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

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

C. Measures

The ~~following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:~~

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Monitoring Responsibility**~~

1.1. Compliance Enforcement Authority

~~**1.1.1**~~ Regional ~~Reliability Organizations~~Entity for Responsible Entities~~.~~

1.1.1 ~~NERC~~ that do not perform delegated tasks for their Regional ~~Reliability Organization~~Entity.

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

~~Annually.~~

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.3~~4~~.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3~~4~~.2 The Compliance ~~Monitor~~Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records ~~for three calendar years.~~and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

~~**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.~~

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

~~2. Levels of Noncompliance~~

~~2.1. Level 1:~~

~~2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,~~

~~2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.~~

~~2.2. Level 2:~~

~~2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,~~

~~2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.~~

~~2.3. Level 3:~~

~~2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,~~

~~2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.~~

~~2.4. Level 4:~~

~~2.4.1 No recovery plan(s) exist; or,~~

~~2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.~~

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

E. Regional ~~Differences~~Variances

None identified.

Version History

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