NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Cyber Security Standards CIP-002-1 through CIP-009-1 Development Highlights

Introduction

On May 9, 2005, NERC posted Draft 3 of its Cyber Security Standards, CIP-002-1 through CIP-009-1, for public review and comment. Sixty-seven sets of comments from sixty-one separate entities were received. The standard drafting team reviewed the comments and, based on that feedback, prepared a final draft for ballot.

This document describes the significant changes made by the drafting team to the final draft as a result of the comments received on Draft 3.

General Changes

The drafting team considered all comments submitted and revised the standards to reflect industry consensus. Overall, the drafting team worked to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly match the requirements, to ensure that requirements are clear and concise, and to eliminate redundancy between the standards.

Global changes affecting all the standards include:

- Throughout the entire set of standards, the phrase “this standard” was changed to “CIP-xxx” (where xxx represents the standard number) to clarify the reference.
- The purpose statement of each of the standards was modified to clarify that the Responsible Entity should use reasonable business judgment when interpreting and applying each of the standards, CIP-002 through CIP-009.
- The word “entities” was removed from item 4.2 in the Applicability section of each standard.
- Measures were rewritten to refer back to the requirement being measured and to ensure the measures do not inadvertently introduce new requirements.

- The Compliance Monitoring Responsibility section of each standard was revised to include references to NERC's compliance monitoring responsibility for the Regions and a third-party's compliance monitoring responsibility for NERC.
- Data retention period for the Responsible Entity was changed from three calendar years to "the previous calendar year."
- In the Additional Compliance Information section, a new 1.4.1 was added to clarify that the Responsible Entity must demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

Definitions of Terms Used in the Standards

The definition of Critical Assets was changed to remove the references to "large quantities of customers" and "significant risk to public health and safety." The new definition is "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." The definition now aligns with CIP-002.

The definition of Physical Security Perimeter was clarified. The phrase "The physical six-wall border surrounding..." has been changed to "The physical, completely enclosed ("six-wall") border surrounding...."

CIP-002-1— Cyber Security — Critical Cyber Asset Identification

Significant changes are:

- The title of this standard was changed to "Critical Cyber Asset Identification" to better reflect the purpose of the standard. Formatting was corrected to number the Purpose section of this standard in accordance with the NERC standard template.
- The list of Required Critical Assets in R1 was removed. R1 was divided into two requirements: "R1. Critical Asset Identification Method" and "R2. Critical Asset Identification." The new R1 requires Responsible Entities to identify and document a risk-based assessment methodology that shall consider, at a minimum, certain assets as listed in the standard. The assets listed for consideration no longer contain references to "IROL" or "80% or greater of the largest single contingency within the Regional Reliability Coordinator." R2 requires Responsible Entities to apply the identified risk-based assessment methodology to identify their lists of Critical Assets.
- "Critical Cyber Asset Identification" was renumbered to R3, the title was changed, the description was modified, and the characteristics of Critical Cyber Assets were clarified regarding the treatment of Control Centers versus generation stations and substations.
- The following was retained from the "Required Critical Asset" list, and are now used as examples of Critical Cyber Assets in R3: 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 requirements to update lists of Critical Assets or Critical Cyber Assets within ninety calendar days of an addition, removal, or modification" were removed.

CIP-003-1 — Cyber Security — Security Management Controls

Significant changes are:

- A requirement for inclusion, in the cyber security policy, of provisions to address emergency conditions was added.
- R1.2 was clarified to indicate that the cyber security policy must be readily available to personnel who have access to, or are responsible for, Critical Cyber Assets.
- A timeframe to review "exceptions" was included.
- The "test" environment was removed from the change management requirements.

CIP-004-1— Cyber Security – Personnel and Training

Significant changes are:

- The update period for Personnel Risk Assessment was extended to 7 years. The review period was changed to be consistent with the update period.
- "Authorized access" was clarified as "authorized cyber or authorized unescorted physical access."
- Personnel risk assessments and training no longer need to be completed prior to permitting authorized cyber or authorized unescorted physical access; rather, they must be conducted within 90 calendars of personnel being granted such access.

CIP-005-1 — Cyber Security — Electronic Security Perimeter

Significant changes are:

- The title of the standard was changed to "Electronic Security Perimeter" to better reflect the purpose of the standard.
- The requirements in R5 for documentation review and maintenance were made consistent with other standards as appropriate.
- Additional language was added to R1 to specifically ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter.
- R1.5 now refers to specific applicable standards and requirements to protect Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter.

- Additional language was added to identify and document Critical and non-critical Cyber Assets within the Electronic Security Perimeter.
- The content of R2 was reorganized, simplified, and clarified.
- Documentation requirements were added to R3 to be consistent with measures, and the language was amended to specify alerting where technically feasible. The language also was amended to account for automated or manual log reviews as compensating measures.
- The requirement for port scanning at the access points in R4 was changed to a review to verify that only ports and services required for operations are enabled.
- R4.3 was amended to require the discovery of all access points to the Electronic Security Perimeter, rather than modems only.

CIP-006-1 — Cyber Security – Physical Security

Please Note: Due to changes made by the drafting team, Requirement numbering has changed. Numbering used in this "Development Highlights" document reflects the numbering in the final draft.

Significant changes are:

- In R1, added that the physical security plan must be approved by a senior manager or delegate.
- Added R1.6 to require Responsible Entities to have procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
- R2.4 and R4 now refer to "other equivalent devices."
- The requirement numbered R2 in Draft 3 was moved into R1, becoming new requirements R1.7 and R1.9. Wording was modified to clarify that the security plan is only required to be updated within 90 days of a change to the security design or configuration, not "any modification of any component."
- The requirement for CCTV monitoring was deleted.
- R2.2: The term "non-reproducible keys" was replaced with "restricted key systems," a more industry standard term.
- R3.1 Alarm Systems: The requirement for alarm monitoring was modified to provide for immediate notification to personnel responsible for responding to an alarm to eliminate confusion over the need for a remote or central monitoring station.
- The following was added in the Additional Compliance Information section: "For dialup accessible critical cyber assets that use non-routable protocols, the Responsible Entity shall not be required to comply with CIP-006 for that single access point at the dial up device."

CIP-007-1 — Cyber Security — Systems Security Management

Please Note: Due to changes made by the drafting team, Requirement numbering has changed. Numbering used in this "Development Highlights" document reflects the numbering in the final draft.

Significant changes are:

- R1 was removed and the introductory paragraph under Requirements was reworded to clarify that CIP-007 applies to all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter.
- R4 has been renamed to Malicious Software Prevention. The requirement to assess anti-virus signatures every thirty days was removed. R4 and its sub-requirements now require that anti-virus and malicious software prevention tools are installed and that a process exists to update the signatures.

CIP-008-1 — Cyber Security — Incident Reporting and Response Planning

The reference to NERC's Indications, Analysis, & Warning Program (IAW) Standard Operating Procedure (SOP) was removed.

CIP-009-1 — Cyber Security — Recovery Plans

No significant changes were made to the requirements of this standard.

Implementation Plan for Standards

The implementation plan has been modified to recognize the time necessary to fully implement these standards. A new phase of compliance has been added to the tables. This new phase is "C" for compliance, which means that a Responsible Entity is in compliance with the requirements of the standards, but has not yet had the time necessary to compile a full calendar year's worth of documentation where necessary. Begin Work (BW) has also been clarified to mean a Responsible Entity has developed and approved a plan to address the requirements of a standard, has begun to identify and plan for necessary resources, and has begun implementing the requirements.