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
Draft 3 Development Highlights
May 9, 2005

Introduction

On January 17, 2005, NERC posted Draft 2 of its Cyber Security Standards, CIP-002-1 through CIP-009-1, for public review and comment. Sixty-three sets of comments from sixty-one separate entities were received. The standard drafting team reviewed the comments and, based on that feedback, prepared Draft 3.

This document describes the significant changes made by the drafting team to Draft 3 as a result of the comments it received on Draft 2.

Changes from Draft 2 to Draft 3

General Changes

The drafting team spent a considerable amount of time ensuring consistency within and across the suite of Cyber Security Standards, matching Requirements to Measures, and eliminating redundancy between the standards. The standard drafting team enlisted two technical editors to assist in its review.

The drafting team modified definitions to improve clarity; for instance, the definition of Physical Security Perimeter has been modified to indicate a six-wall boundary.

References in CIP-003-1 through CIP-009-1 pertaining to exceptions have been clarified. The revised language states that a Responsible Entity may approve and document exceptions to its Cyber Security Policy, not NERC standards. Specific language has been added to CIP-006-1 and CIP-008-1 limiting the ability to write exceptions in several policy areas. All allowable exceptions must be documented and approved as specified in Requirement R3 of CIP-003-1.

Other changes across the suite of standards include:

- These standards are now applicable to the offices of NERC and Regional Reliability Organizations;
- Language that exempts from these standards facilities regulated by the U.S. Nuclear Regulatory Commission and the Canadian Nuclear Safety Commission has been clarified;
- Language has been added to clarify that communication networks and communication links between discrete Electronic Security Perimeters are exempt from these standards; and,
- Language has been added to link the CIP-002-1 through CIP-009-1 together as a package.

Cyber Security – Critical Cyber Assets – CIP-002-1

The purpose statement has been revised to better describe the intent of the standard, the increased need for cyber security, and the general requirements of the standard.

Critical Assets in Requirement 1 have been split into Required Critical Assets impacting the reliability or operability of the bulk electric system and Additional Critical Assets identified using risk-based assessment by the Responsible Entity.

The Requirement for updating the Critical Asset and Critical Cyber Asset list has been changed to 90 days from 30 days.

The Requirement to list non-critical assets on the same network as critical assets has been removed and the Requirements to protect non-critical assets within the Electronic Security Perimeter have been moved to CIP-005-1.

Requirements for Critical Cyber Assets with dial-up access and not using a routable protocol have been moved to CIP-005-1.

Cyber Assets at a substation or generating station using a routable protocol that does not extend through the electronic security perimeter, and without direct dial-up access, will not be identified as Critical Cyber Assets.

The review and approval of the Critical Asset and Critical Cyber Asset lists by a senior manager has been revised to be done annually.

The standard recognizes that a Responsible Entity may determine it has no Critical Assets or Critical Cyber Assets. If such a determination is made, the Responsible Entity must document that determination to show compliance with this standard.

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

Draft 2 incorrectly introduced new Requirements in the Measures section. Draft 3 corrects this error and matches Requirements to Measures. In response to several comments, titles have been added to all top-level requirements for clarity. The Levels of Non-compliance section has been revised.

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

Levels of Non-compliance were modified to address issues raised in public comments.

Cyber Security – Electronic Security – CIP-005-1

Requirement R1 has been broken into sub-requirements for clarity. Requirement R1 now also includes a sub-requirement to provide the same Electronic Security Perimeter protections to Cyber Assets used to implement access controls and monitoring of the Electronic Security Perimeter(s).

Requirement R2 from Draft 2 (network ports and services) has been moved as a sub-requirement (R2.1) of an overall Access Control requirements section R2 in Draft 3.

Requirement R3 from Draft 2 (access control for modems) has been moved as a sub-requirement (R2.3) of an overall Access Control requirements section R2 in Draft 3.

The Requirement for strong access controls for external interactive access to the Electronic Security Perimeter has been clarified. References to specific technologies have been removed and are more appropriately addressed in the FAQ.

For clarity, Requirement R3 includes sub-requirements for reviewing authorized access on a periodic basis where monitoring cannot be implemented or can only be partially implemented.

The requirements for vulnerability assessment of the access points to the Electronic Security Perimeters, originally included in CIP-007-1, have been moved to this standard for consistency.

Corresponding changes to the Measures and Levels of Non-compliance were made.

Cyber Security – Physical Security – CIP-006-1

The Requirement for defining physical access controls of a security cage has been removed. The access controls for a security cage should be addressed in the physical security plan as a perimeter.

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

References to attended and unattended facilities have been removed. Titles for the following Requirements have changed; Account and Password Management changed to Account Management, Operating Status Monitoring Tools changed to Security Status Monitoring, Integrity Software changed to Anti-Virus Software, and Identification of Vulnerabilities and Responses changed to Cyber Vulnerability Assessment. Requirements for non-critical assets within the Electronic Security Perimeter have been added to this standard.

Test Procedures and Account Management Requirements have been broken out into separate sub-requirements. What constitutes “significant changes” for Test Procedures has been clarified. The Requirements for Patch Management and Anti-Virus Software have been updated for clarity. The Requirement for Cyber Vulnerability Assessment was updated to clarify the intent. The Requirement for Ports and Services was clarified to apply to devices inside the Electronic Security Perimeter (those devices on the Perimeter are addressed in CIP-005.)

A Requirement was added specifying that field devices without electronic access controls shall have physical access controls. A Requirement for protection of Critical Cyber Assets disposed or redeployed was added. Requirements for Documentation Review and Maintenance were added. The Measures and Levels of Non-compliance were updated to reflect the updated Requirements.

The stand-alone Requirement for Retention of System Logs was removed and the retention requirement added as a sub-requirement in the appropriate Requirements. Requirements for Configuration Management were removed from CIP-007 as they are addressed in CIP-003. The Backup and Recovery requirement was moved to CIP-009.

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

The definition of Cyber Security Incident has been updated to clearly include the Electronic Security Perimeter. References to “incident” were changed to “Cyber Security Incident” as appropriate. Testing the Incident Response Plan has been added as a requirement.

Cyber Security – Recovery Plans – CIP-009-1

Language has been added to address backup of information critical to successful restoration of Critical Cyber Assets.

Implementation Plan for Standards

Draft 2 of the implementation schedule has been significantly modified to recognize the time necessary to fully implement these standards. This includes the recognition that any undertaking of this scope requires first developing a plan to outline a Responsible Entity's implementation strategy. With this in mind, Draft 2 of the Implementation Plan includes a new phase of implementation referred to as "Begin Work." This phase represents the finalization of a Responsible Entity's plan to address a given Requirement in the standards.

The Implementation Plan has been divided into three separate tables to recognize three separate groups of Responsible Entities:

(1) Balancing Authorities and Transmission Operators that were required to self-certify compliance to NERC's Urgent Action Cyber Security Standard 1200 (UA 1200), and Reliability Coordinators;

(2) Transmission Operators and Balancing Authorities that were not required to self-certify compliance to UA Standard 1200, Transmission Providers, and the offices of NERC and the Regional Reliability Organizations.

(3) Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators, and Load-Serving Entities.

Entities in the first two groups have registered per the Functional Model. Entities in the third group, although most likely identifiable, have yet to register to the model and, as such, are not currently included in the NERC Compliance Program.

For Responsible Entities in the first two groups, the implementation plan requires Auditable Compliance to all Requirements by second quarter 2009. For Responsible Entities in the third group, the implementation plan requires Auditable Compliance to all Requirements within 36 months of the registration to a Functional Model function.