Critical Infrastructure Protection — Cyber Security Standards
Development Highlights
January 17, 2005

Introduction

On August 13, 2003 the NERC Board of Trustees approved the implementation of Urgent Action Cyber Security Standard 1200 (UA 1200). Because an Urgent Action standard expires after one year, with the opportunity to extend the standard for only one additional year, an effort to replace UA 1200 with a permanent standard began even before the NERC Board approved Urgent Action Standard 1200.

A Standard Authorization Request (SAR) drafting team was appointed on June 16, 2003 to develop the scope of the permanent standard. The SAR was posted twice for industry comment, once from July 1 through August 8, 2003 and again from December 1, 2003 through January 21, 2004. On April 7, 2004 the NERC Standards Authorization Committee (SAC) approved the SAR for Standard 1300 and approved a drafting team to develop the standard. The drafting team represents a broad spectrum of the electric utility industry in North America with recognized experts in cyber and physical security.

The stated purpose of the permanent standard is to "to protect the critical cyber assets (hardware, software, data, and communications networks) essential to the reliability of the bulk electric system." Draft 1 of Standard 1300 was posted for public comment on September 15, 2004. The standard drafting team evaluated approximately 700 pages of comments representing almost 430 separate comments from more than 70 separate entities. The team then used the combined expertise of the team members to interpret the comments from industry and to prepare draft 2 of the standard.

This document reviews the changes made to the standard in draft 2 as a result of the comments received on draft 1. It also discusses the changes made as a result of the continuing evolution of the NERC standards development process.

Changes from Urgent Action Standard 1200

The drafting team members discussed the implementations of UA 1200 within their organizations. Their experiences led them to condense the number of sections in the draft Standard 1300 to eight from the UA 1200's original 16. The team also revised for clarity the definitions in response to many comments NERC received during the balloting and reballoting of UA 1200. The other significant change from UA 1200 to Standard 1300 was the expansion of the scope, which now includes for consideration those cyber assets at locations/facilities other than an entity's control center.

New items in Standard 1300 that were not in UA 1200 include a requirement for a formal governance process. It also requires authorization to place into production and it includes additional requirements concerning the access authorization process. Other additions include

generic account management, change control and configuration management, operating status monitoring tools, and backup and recovery.

The drafting team made many changes to improve the clarity of requirements and measurements.

Changes due to NERC's Standards Process Evolution

Subsequent to the posting of draft 1 of Standard 1300 for public review and comment, NERC introduced a new format for its standards. At the same time, NERC introduced a new alpha-numeric identification scheme for its standards. NERC's new format does not provide for sections within a standard.

After consideration of the new format, and in agreement with the NERC Director of Standards, draft 1 of Standard 1300 was divided into eight separate standards corresponding to the eight sections in draft 1. These new draft standards were assigned numbers consistent with the new alpha-numeric standards identifier. The table below maps the sections of Standard 1300 draft 1 to the new draft 2 CIP standards.

Old Section #	Topic	New Std #
1301	Security Management Controls	CIP-003-1
1302	Critical Cyber Assets	CIP-002-1
1303	Personnel and Training	CIP-004-1
1304	Electronic Security	CIP-005-1
1305	Physical Security	CIP-006-1
1306	Systems Security Management	CIP-007-1
1307	Incident Reporting and Response Planning	CIP-008-1
1308	Recovery Plans	CIP-009-1

Changes Based On Industry Comments

General Changes

The standards were reformatted and modified for clarity and consistency. All eight standards now include a statement in their applicability sections that specifically exclude nuclear facilities.

A statement added to the applicability section of standards CIP-003-1 through CIP-009-1 exempts applicable entities that have no critical cyber assets from complying with these standards. This assumes that all applicable entities have conformed to the requirements of CIP-002-1 to make their determinations of critical cyber assets. This applicability exemption recognizes that some entities to whom the standards would otherwise apply may find they have

no critical cyber assets as determined by compliance with standard CIP-002-1. In this case, those entities would not be required to comply with the requirements of standards CIP-003-1 through CIP-009-1.

Changes to the definitions include:

- "Bulk Electric System Asset" was replaced by the Version 0 standards term "Bulk Electric System."

- The definition of "Critical Asset" is now the same as the one found in NERC's Physical Security – Substation Guideline. This change was made to assist responsible entities in identifying assets critical to bulk electric system grid operation.

- The definitions of "Incident" and "Security Incident" were replaced with a new definition for "Cyber Security Incident."

- The definition of Critical Cyber Assets has been revised.

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

This standard was modified to more clearly state the point that critical assets are those that provide critical operating functions and tasks affecting the interconnected bulk electric system. The standard includes a list of such operating functions and tasks.

The inclusion criteria for generation resources and generation control centers were changed to 80% or greater of the largest single contingency within the applicable Regional Reliability Organization.
This standard now requires the documentation of all other cyber assets that exist within the same electronic perimeter as a critical cyber asset and requires the protection of those assets to ensure the security of the critical cyber asset.

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

Change Management requirements were moved into this standard from standard CIP-006-1.

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

"Background Screening" was changed to "Personnel Risk Assessment" and the section was expanded to be more inclusive in application.

Social Security Number verification was changed to "Identity Verification" to provide for legal variance between United States and Canadian laws.

"Unrestricted access" was changed to "authorized access" throughout for consistency and clarity.

Access revocation and records change requirements under this section were changed throughout to "7 calendar days for normal changes in status, and 24 hours for personnel terminated for cause."

Although it received a number of comments asking that drug screening be included as a requirement in this section, the drafting team elected not to do so. However, the team notes that entities are not precluded by this standard from implementing a drug screening program.

Cyber Security – Electronic Security – CIP-005-1

Electronic Access Control now includes a list of options to help clarify the requirement for strong technical and procedural controls for interactive access to the perimeter. A technical feasibility caveat also has been added to the requirement for log-on banners for interactive access.

Cyber Security – Physical Security – CIP-006-1

Based on comments received in response to draft 1, the requirements section was updated to more clearly define the physical security elements of the entity's Security Plan. Also, the Physical security perimeter requirement was clarified, removing references to assigned security levels, and modifying the four-wall boundary concept. The requirement for CCTV monitoring control was modified to include the point of facility access as a monitoring point. Manual logging control was modified to include remote verification as a means of ensuring completeness.

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

Draft standard CIP-007-1 now includes a reference to "unattended facilities" and provides a clear delineation of the requirements that apply to attended and unattended faciltities.

The concept of risk based assessment was introduced to the Security Patch Management section.

Retention of System Logs now clearly states that it is the responsible entity who must determine its logging strategy.

References to penetration testing were removed and vulnerability testing was more clearly defined.

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

The title of standard CIP-008-1 was changed to **Incident Reporting and Response Planning** to better reflect the scope of this standard. The introductory paragraph was modified to clarify the purpose of this standard. The Cyber Security Incident Reporting requirement was updated to reflect that the responsible entity is accountable for ensuring that the Electricity Sector Information and Analysis Center (ES ISAC) receives all cyber security incident reports. If a cyber security incident occurs and is not reported to the ES ISAC it will now result in a level three noncompliance.

Cyber Security – Recovery Plans – CIP-009-1

The third paragraph was moved to the FAQ as it primarily explained the degree of recovery required in consideration of the expected impact and risk involved. The requirement to 'post' a recovery contact list was removed.

Implementation of Standards

The standard drafting team believes that a transition period for implementation of the requirements of cyber security standards is appropriate. A draft implementation plan is posted with draft 2 of the standards for industry review and comment. This implementation plan includes a table that describes how compliance to the requirements of Standards CIP-002-1 through CIP-009-1 are to be phased in. The draft implementation plan posted with draft 2 of the cyber security standards assumes approval by the Registered Ballot Body and the NERC Board of trustees by early September 2005.