NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Development Overview

CSSDTO706

Meeting with FERC Technical Staff

July 28, 2011

to ensure the reliability of the bulk power system

Objectives

- Historical Timeline
- CIP-002-4
- CIP-005-4
- CIP Version 5

Project 2008-06 Overview

- **FERC Order 706**
- SDT appointed – August 2008
- CIP Version 2 – September 2009
- CIP Version 3 – March 2010
- CIP Version 4 – Ongoing Effort

CSO706 SDT Members

- 17 members – almost all asset owners
- Representation from IOUs, US and Canadian Government, Cooperatives, Municipals, Independent Power Producers, and ISO/RTO
- Worked together for 3 years
- Monthly face-to-face meetings, several interim conference calls and multiple webinars/workshops
- Worked through 3 successful ballots

CIP-002-4 Overview

- Version 4 of the CIP Standards
- Approved by Industry December 30, 2010
- Submitted to FERC February 10, 2011
  - 2,232 page filing
  - http://www.nerc.com/files/Final_Final_CIP_V4_Petition_20110210.pdf
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

CIP-002-4 Overview (cont.)

- Replaces “risk-based assessment methodology” with “bright-line criteria”
  - Still maintains the concept of Critical Asset and Critical Cyber Asset
  - Uniform application across all entities and regions
  - Eliminates subjectivity by entities over what is “critical”
  - 17 defined criteria
  - To the greatest extent possible, bright line criteria tied to operational standards

CIP-002-4 Applicability

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by 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 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

CIP-002-4 Effective Date

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

CIP-002-4 Requirement R1

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

CIP-002-4 Requirement R2

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1

CIP-002-4 Requirement R3

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 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 list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Remote Access UA

- Implements requirements on “Cyber Assets” used for “monitoring or support” of Critical Cyber Assets when communication is initiated from outside an Electronic Security Perimeter
  - i.e., remote laptop or desktop systems accessing Critical Cyber Assets, but *not* for the purpose of control
  - Remote access for the purpose of control is the subject of CAN-0005
- Development now integrated into CIP Version 5

CIP V5

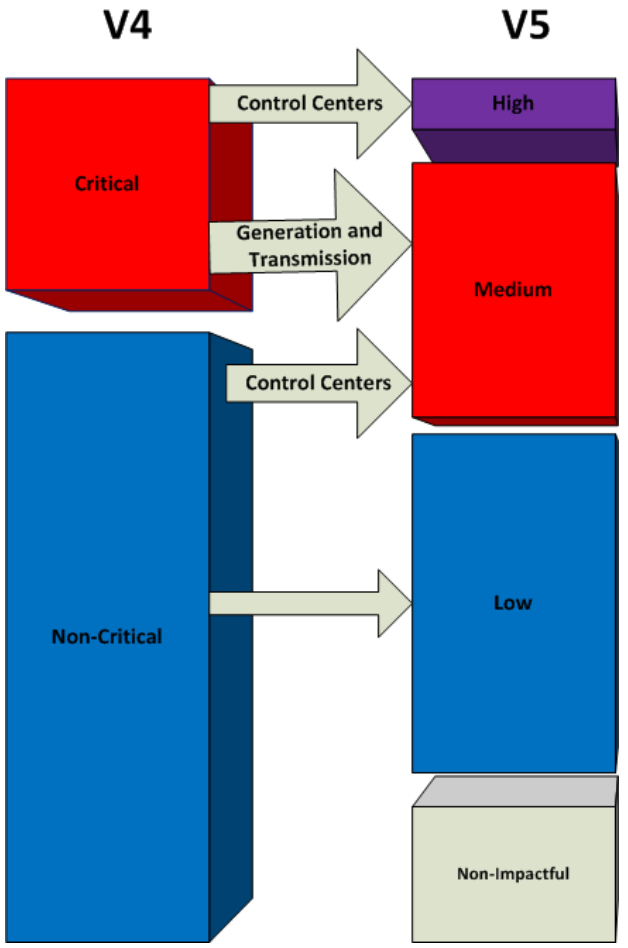
- The Drafting Team continues to work to address the remaining issues in Order 706
  - Using the “CIP-002 to CIP-009 +” organization
  - Monthly meetings and many conference calls
  - Initial ballot by December 2011
- The Drafting Team developed a set of development goals

Development Goals

Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.	**Goal 5**: To minimize technical feasibility exceptions.
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.	**Goal 6:** To develop requirements that foster a “culture of security” and due diligence in the industry to complement a “culture of compliance”.
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements.	

Levels of impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection



Example Format

R1. Each Responsible Entity shall implement a cyber security governance structure that includes the required items in CIP-011-1 Table R2 – Security Governance.

Rationale: *One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.*

Summary of Changes: *[Use this section to describe any broad changes applying to multiple rows in the table or removed requirements. These changes require the same level of justification as in the table rows. If all changes can be sufficiently described in the table rows, then this section can be omitted.]*

Additional Guidance: *The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs.*

2. Rationale

3. Requirement-level change justification

4. Additional Guidance

5. Applicability

6. Requirement

7. Measurement

	CIP-011-1 Table R1 – Security Governance and Policy		
	Applicability	Each Responsible Entity shall include the following in their Account Management Documentation:	Measurement
1.1	Low	Identify a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard	Acceptable evidence may include documentation that identifies a single senior management official.
Reference to prior version: CIP-003 R1		**Change Justification:** Removed prescriptive requirement of how manager must be identified. Removed requirement regarding delegation. Requirement to update this within 30 days was removed. Requirement to authorize and document exceptions from the cyber security policy removed.	

8. Reference to Prior Version

9. Row-level Change Justification

Requirement Filters

- Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? If these questions cannot be answered, is the requirement necessary?
- Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? If so, the requirement may be too specific.
- Is the timeframe arbitrary?
- Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Thank you

to ensure the reliability of the bulk power system