CIP Cyber Security Standards
Development Update

John Lim – Consolidated Edison Co. of New York
Rob Antonishen – Ontario Power Generation
Disclaimer

This NPCC TFIST workshop provides a forum for the presentation and discussion of member experience in the implementation of compliance programs for the NERC CIP Cyber Security Standards. Materials presented or discussed are the presenters’ own interpretation and recommendations and do not necessarily represent those of their organizations or NPCC.
Agenda

- Development Process Changes
- CIP-002-4
- CIP-005-4 Urgent Action
- CIP-10 and CIP-011
CIP Standard Development Process

- Approved by NERC Standards Committee

- Informal Comments
  - Forms
  - Webinars
  - Workshops
  - Other venues (regional meetings, etc.)
  - Formal response to each comment not required
CIP Standard Development Process (2)

- **Formal Comments (45 days)**
  - Concurrent Ballot Pool formation/Pre-Ballot Review (1st 30 days)
  - Ballot (Last 10 days)
  - All comments must be responded to.

- **Re-ballot**
  - Can make changes to standard between ballots
  - As many as required for consensus
What Has Been Completed

  - Phase 1
  - Low Hanging Fruits for FERC 706 Directives
  - Became Effective 4/2010

- **Version 3 (CIP-002-3 – CIP-009-3)**
  - 90 day FERC directed changes to Version 2
  - Effective 10/2010
What’s In Progress

- **CIP-002-4**
  - 1st formal posting/concurrent ballot: September 2010
  - Target: Complete by 12/2010

- **CIP-005-4**
  - Urgent Action: Response to Remote Access Vulnerability
  - Separate Drafting Team
  - Posted for Comment/Ballot: 08/18/2010
  - Intent to File to FERC with CIP-002-4 package

- **CIP-10 & CIP-011**
  - Concept Paper: July 2009
  - Informal Posting: CIP-002-4 12/2009 (not the same as the current CIP-002-4)
  - Informal Posting: CIP-010 and CIP-011 07/2010
  - Target: 2011
CIP-002-4

- **CIP-002-4 – Narrow Scope**
  - Non-uniform application of methodologies for identifying Critical Assets, resulting in wide variation in the types and number of critical assets across regions.
  - Replace the Entity defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
  - FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). Requirement for oversight is significantly mitigated.
  - External perceptions of insufficiency of the Entity defined methodologies in identification of Critical Assets.
CIP-002-4 Schedule

- Sep 20
  - Posting for Comment and Ballot

- Oct 25
  - Ballot Opens

- Nov 4
  - Ballot Closes
  - Comments Due

- Nov 5 – 18
  - Drafting Team Responds to Comments
  - Incorporates Changes

- Nov 19 – 30
  - Second Ballot
Posted Documents – CIP V4 Standards

- CIP-002-4
  - Main revisions
- CIP-003-4, CIP-004-4, CIP-006-4, CIP-007-4, and CIP-008-4, CIP-009-4
  - Conforming changes
- Implementation Plan
- Reference (Guidance) Document
- Mapping Document
- VRF/VSL Analysis
- Summary Response to CIP-010 Attachment 2
  - “Consideration of Comments on Question 7”
CIP-002-4

- Replace Risk-Based Methodology with Bright-line Criteria (R1 & Attachment 1)
  - Generation
  - Transmission
  - Control Centers
- Minor changes to R2 – Identification of Critical Cyber Assets
- No changes to CIP-003-CIP-009 except conforming changes
- Reference Document and Implementation Plan
Requirement R1

Critical Asset Identification — Each 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 I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.
Requirement R2

Critical Cyber Asset Identification —..... 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 adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes.......

- V3 qualifications still apply
Requirement R3

Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets.....

- No change in the requirement substance
Attachment 1

- Criteria for Identification of Critical Assets (BES)
  - Bright-lines
- Generation
- Transmission
- Control Centers
- Anything else the Responsible Entity wants to include
Generation

- Plants with group of units = or > 1500 MW
  - Single unit or multiple unit plants
  - Critical Cyber Assets: Aggregate Impact
  - Nuclear Facilities evaluated based on bright line

- Required to run for reliability reasons
  - Designated by Transmission Planners

- Blackstart Resources
  - Designated by Transmission Operator in its restoration plan
  - Initial Plant for restoration – Glossary Term defined and used by EOP-005-2
Transmission

- Reactive resources = or > 1000 MVARs
- Cranking Paths up to multiple path options
- Operating at = or > 500 KV
- Operating at = or > 300 KV with 3 other stations
- Facilities, if lost, etc., would violate IROLs
- FACTS, if lost, etc., would violate IROLs
- Loss of Critical Generation
- Nuclear Plant Interface Requirements (NPIRs)
- SPS/RAS, if lost, etc., would result in IROLs
Control Centers

Primary and Backup

- Performing the functional obligations of RC, BA, TOP
  - Refer to Reference Document for delegated functions (TOs)

- Generation Control = or > 1500 MW in a single interconnection
Any additional assets that the Responsible Entity deems appropriate to include
Version 4: Implementation Timeline

All dates included in the timeline are purely speculative and are for example purposes only.
CIP-005-4

- Urgent Action Process
- Addresses Remote Access vulnerability
- Counterpart to CAN-005
- Remote Access for Support and Maintenance
- Formal comments and Pre-ballot Review: 8/18/2010 to 9/17/2010
- Ballot: 9/17
CIP-005-4 Schedule

- Pre-ballot posting and formation of ballot pool closed on 9/17/2010
- Balloting started on 9/17/2010 for 10 days
- Likely withdraw CIP-005-4 in response to ballot comments – modify and re-post for initial ballot
- Schedule to complete for concurrent approval and filing of CIP-002-4 with regulators at the end of the year
CIP-010

- Categorized list of BES Cyber Systems
- Based on Impact on Functions
  - High
  - Medium
  - Low
- Basis for Application of Appropriate Controls (CIP-011)
- Formal Comment: 7/2011
CIP-011

- Posted for informal comment May 2010
- SDT reviewed comments and feedback received at the May 2010 workshop in Dallas.
- SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-011 by the initial target date of December 2010.
- Efforts on updating CIP-011 have been substantially deferred, with plans to resume in December. Efforts to review and respond to comments has continued.
CIP-011 Scope and Objectives

- Address FERC Order 706 Directives:
  - 2 or more diverse security measures for defense in depth at the security boundaries
  - Active vulnerability assessments every 3 years
  - Incorporate forensic data collection and procedures

- Consideration of adapting the NIST Security Risk Management Framework
CIP-011 Structure

- The SDT requested feedback on the new CIP-011 format:
  - Keep CIP-011-1 as one standard
  - Break CIP-011-1 up into multiple standards
  - No Preference

- Industry response:
  - No preference (1/3 – 1/3 – 1/3)
CIP-011 Guiding Principles

- Policy focuses on high-level subject areas.
- To draft standards at a higher level to minimize the need for TFEs.
- STD will attempt to preserve the effort invested by Responsible Entities by developing a mapping from the existing standards 003-009 to 011.
CIP-011 Sub-Teams

- **Personnel and Physical Security:**
  - Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
  - (FERC: Drew Kittey)

- **System Security and Boundary Protection:**
  - Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff
  - (Observer Participant: Brian Newell)
  - (FERC: Justin Kelly)
CIP-011 Sub-Teams (cont.)

- Incident Response and Recovery:
  - Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson
  - (Observer Participant: Jason Marshall)
  - (FERC: Dan Bogle)

- Access Control and Boundary Protection:
  - Sharon Edwards (Lead), Jeff Hoffman, Frank Kim, Jerry Freese
  - (Observer Participants: Roger Fradenburgh, Sam Merrell)
  - (FERC: Mike Keane)
CIP-011 Sub-Teams (cont.)

- Change Management, System Lifecycle, Information Protection, Maintenance, and Governance:
  - Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters
  - (Observer Participant: Brian Newell)
  - (FERC: Jan Bargen, Matthew Dale)
What should you be doing?

to do
Questions or Comments?