NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Revisions

Standard Drafting Team Update

June 19, 2014, 1 pm – 3 pm EDT
Industry Webinar

RELIABILITY | ACCOUNTABILITY




Administrative Items

- NERC Antitrust Guidelines
  - It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Agenda

- Overview of FERC Directives
- Overview of Development Activities
- Overview of Revisions
  - Identify, Assess, and Correct – struck from 17 Requirements
  - Low Impact Assets – revised CIP-003
  - Communication Networks – revised CIP-006 & CIP-007
  - Transient Devices – revised CIP-004 & CIP-010
- Implementation Plan
- Next Steps

Overview of FERC Directives

- FERC approved CIP V5 standards in January 2014.
- FERC directed NERC to modify certain aspects:
  - Identify, Assess, and Correct language
  - Communication Networks
  - Low Impact Assets
  - Transient Devices
- Identify, Assess, and Correct and Communication Networks modifications must be filed at FERC by February 3, 2015.

Overview of Development Activities The Team

- Standard Drafting Team (SDT) appointed to address these revisions in Project 2014-02.
  - Maggy Powell, Exelon
  - Philip Huff, AECC
  - David Revill, GTC
  - Jay Cribb, Southern Company
  - Forrest Krigbaum, BPA
  - David Dockery, AECI
  - Greg Goodrich, NYISO
  - Christine Hasha, ERCOT
  - Steve Brain, Dominion
  - Scott Saunders, SMUD

Overview of Development Activities Key Objectives

- Four directive areas
- One year filing deadline
- Outreach during development and comment period

Overview of Development Activities Work Schedule

- SDT and observers participated in aggressive development schedule
  - Ten hours of conference calls per week, including subgroup calls focused on each directive area
  - Four face-to-face SDT meetings
- Participation from variety of stakeholders ensured that the SDT considered different perspectives from industry, government, and NERC
- Met the June 2 target posting date for initial comment and ballot

Identify, Assess, and Correct

- Identify, Assess, and Correct language struck from all 17 requirements
  - SDT determined that the requirements should state the performance expectation and compliance language should be removed
- Substantive requirements remain the same
- Violation Severity Levels revised accordingly

Identify, Assess, and Correct

- SDT continues coordination with NERC Compliance and Enforcement Staff on supporting documents
  - NERC presented to the SDT initial draft RSAWs for CIP-002, CIP-007, and CIP-009 at the May meeting
  - The NERC RSAW development team continues to prepare draft RSAWs for concurrent posting with revised CIP V5 standards
  - SDT suggested scenarios for NERC to help illustrate how RAI is applied
  - SDT provided "Frequently Asked Questions" (FAQ) for NERC response to offer insight on the relationship between RAI and the removal of IAC
  - NERC posted the FAQ document on the project page
- There will be a webinar on RAI today at 3 pm EDT

Identify, Assess, and Correct

- FAQ Excerpts:
  - Intent of IAC was to shift compliance and enforcement activities to focus on areas of risk along with effective governance and business practices and implementing corrective action
  - RAI seeks to reduce administrative burden associated with high frequency security obligations in CIP requirements by allowing entities to log minimal risk non-compliance, with presumption of enforcement discretion
  - RAI will not change CIP compliance obligations but will address how areas of non-compliance will be assessed and resolved

Identify, Assess, and Correct

- FAQ Excerpts (continued):
  - Removal of IAC means entities no longer have to incorporate IAC into their compliance programs
  - Compliance exceptions are non-compliance that is not to be pursued through enforcement. It represents the exercise of enforcement discretion
  - Entities qualify for compliance exceptions if they pose a minimal risk to the reliability of the Bulk Electric System
- Read the complete FAQ document posted on the CIP V5 Revisions project page under Supporting Documents
- Attend webinar at 3 pm EDT today on RAI

Low Impact Assets

- CIP-003-6 Requirement R2 now in table format
  - SDT kept all requirements applicable to low impact assets in this requirement
  - Technical areas same as CIP-003-5 passed by industry but with more specificity to meet FERC directive
  - Proposed requirement language borrowed from existing, FERC- and industry-approved V5 standards but tailored to low impact
- Parent requirement above table parts is as follows:

R2. Each Responsible Entity for its assets containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table.

Low Impact Assets

- CIP-003-6 Requirement R2, Part 2.1
  - Similar to Requirement R2 passed by industry in CIP-003-5

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.

Low Impact Assets

- CIP-003-6 Requirement R2, Part 2.2

2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).

Low Impact Assets

- CIP-003-6 Requirement R2, Part 2.3

2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have external routable protocol paths.

Low Impact Assets

- CIP-003-6 Requirement R2, Part 2.4
  - SDT drew from CIP-005-5 when developing controls but tailored them to low impact assets

2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

Low Impact Assets

- CIP-003-6 Requirement R2, Part 2.5
  - SDT drew from CIP-008-5 for requirements but tailored them to lows

2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

Low Impact Assets

- CIP-003-6 Requirement R2, Part 2.6

2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Communication Networks

- CIP-006-6 Requirement R1, new Part 1.10
  - Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same ESP in those instances when such cabling and components are located outside of a PSP
  - Where physical access restrictions are not implemented, entity shall document and implement:
    - Encryption of data
    - Monitoring the status of the communication link and issuing an alarm
    - Equally effective logical protection
  - Applicable to High Impact BES Cyber Systems and PCAs and Medium BES Cyber Systems at Control Centers and PCAs

Communication Networks

- CIP-007-6 Requirement R1, Part 1.2: new applicability and incorporated new glossary term

CIP-007-~~5~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Transient Devices – New and Modified Definitions

- **Transient Cyber Asset** - A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
- **Removable Media** - Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.
- 30-day exemption removed from **BES Cyber Asset** and **Protected Cyber Asset** definitions

Transient Devices

- CIP-010-2 new Requirement R4
  - New Table Requirement
  - Addressed the FERC directive to consider the following security controls:
    - device authorization as it relates to users and locations
    - software authorization
    - security patch management
    - malware prevention
    - detection controls for unauthorized physical access to a transient device
    - processes and procedures for connecting transient devices to systems at different security classification levels
  - Borrowed concepts from FERC- and industry-approved V5 standards

Transient Device Protection

- CIP-010-2, Requirement R4, Part 4.1 (Authorization)

4.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. Authorization shall include: 4.1.1. Users, individually or by group/role; 4.1.2. Locations, individually or by group/role; 4.1.3. Defined acceptable use; and 4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or • A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.

Transient Device Protection

- CIP-010-2, Requirement R4, Parts 4.2 and 4.3 (Malware Protection)

4.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).

4.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).

Transient Device Protection

- CIP-010-2, Requirement R4, Parts 4.4 and 4.5 (Malware Protection) (continued)

4.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
4.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Transient Device Protection

- CIP-010-2, Requirement R4, Parts 4.6 (Unauthorized Modifications)

4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4. For a modification that deviates from the state in Part 4.1.4, either: • Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or • Update Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.

Transient Device Protection

- CIP-010-2, Requirement R4, Part 4.7 (Security Patches)

4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date. For security patches that are not up-to-date, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

Transient Device Protection – Modification to Other Standards

- CIP-004-6 – Adds Transient Cyber Assets and Removable Media to cybersecurity training program in Requirement R2, Part 2.1
- CIP-007-6 – Added clarifying language in guidance for Requirement R3 (malware protection) to remind entities of the Transient Device Protections in CIP-010-2, Requirement R4
- CIP-011-2 – Added qualifiers to guidance for entities to include Transient Cyber Assets and Removable Media in their information protection programs

Implementation Plan

- Builds from April 1, 2016 effective date of V5
- While the standard has an effective date, a compliance date may differ for Requirements
- V5 IAC language is not expected to go into effect
- The following from V5 implementation remains the same:
  - Initial performance of certain periodic requirements
  - Previous identity verification
  - Planned or unplanned changes resulting in a higher categorization

Implementation Plan

- For requirements and parts not listed below, the compliance date would be the effective date of standard proposed to be later of April 1, 2016 or 3 months following govt. approval

Standard	Requirement	Proposed Implementation Periods
CIP–003–6	**R2**	Later of April 1, 2017 or 9 months following govt. approval.
CIP–006–6	**R1**	Part 1.10 – Effective Date plus 9 months
CIP-007-6	**R1**	Part 1.2 – Applicable non-programmable electronic equipment associated with new BES Cyber Systems – Effective Date plus 6 months
CIP-010-2	**R4 (new)**	Effective Date plus 9 months

Posting Schedule

- NERC Standards Committee authorized posting for 45-day comment and ballot on May 30
- Comment period open June 2-July 16
- Join the ballot pool from June 2-July 2
- Reliability Standards Audit Worksheets (RSAWs) posted June 17
  - NERC collects comment separately from the standard revision comments
  - SDT is not part of the RSAW comment review process
- Ballot period open July 7-16
  - CIP V5 Revisions will use the current ballot and commenting system

Next Steps

- SDT will consider all comments and make appropriate revisions
- SDT meeting July 29-31 in St. Paul, MN
- SDT meeting week of August 19 in San Francisco, CA
- CIP V5 Revisions project page: http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx

Comment Form

- SDT poses eight questions for comment
- SDT encourages industry to provide constructive input for revisions with justification for the changes
- Constructive input allows for the SDT to consider the comments and respond accordingly
- Submit comments of support regarding the SDT's direction in addressing all four directives

Related Items

- BES Cyber Asset Survey posted for 45-day industry comment period until July 14, 2014
  - Posted on Project 2014-02 project page
  - Submit comments via email and attachments are accepted to BESCyberAssetSurvey@nerc.net
- RSAWs posted for industry comment until July 16, 2014
  - Submit comments via email to RSAWfeedback@nerc.net

Questions and Answers