NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Revisions

Standard Drafting Team Update

Industry Webinar

April 22, 2014: 10:00am - 12:00pm ET

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Topics

- FERC Order 791 Highlights
- Standard Drafting Team (SDT) Introductions
- Where the team is today on the directives
- Implementation Plan
- Next steps
- Questions and answers

FERC Order 791 Highlights

- Directed changes to four main areas:
  - Identify, Assess, and Correct – Filing deadline Feb. 3, 2015
    - Remove or modify the IAC language, retain the substantive provisions, and clarify the obligations for compliance
  - Communication Networks – Filing deadline Feb. 3, 2015
    - Define communication networks and create new or modified Reliability Standards to protect the nonprogrammable components of communication networks (e.g. cables and wires)
  - Low Impact Assets – No filing deadline
    - Add objective criteria from which to judge the sufficiency of controls
  - Transient Devices – No filing deadline
    - Develop new or modified Reliability Standards for transient devices (e.g. thumb drives and laptops)

SDT Introductions

Full Team

- 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

Sub-Group Assignments

Identify, Assess, and Correct
Leads: Greg Goodrich, Scott Saunders
Support: Maggy Powell, Ryan Stewart

Communication Networks
Leads: David Revill, David Dockery
Support: Philip Huff, Marisa Hecht

Low Impact Assets
Leads: Jay Cribb, Forrest Krigbaum
Support: Maggy Powell, Marisa Hecht

Transient Devices
Leads: Steve Brain, Christine Hasha
Support: Philip Huff, Ryan Stewart

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Low Impact Assets

RELIABILITY | ACCOUNTABILITY




Treatment of Lows Original Language

CIP-003-5

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

Treatment of Lows Order 791

Order 791 Summary – Low Impact Assets

"… requiring NERC to address the lack of objective criteria against which NERC and the commission can evaluate the sufficiency of an entity's protection of low impact assets." (pg. 62, para. 108)

- Requiring specific controls for Low Impact assets, including subdividing the assets into different categories with different defined controls applicable to each subcategory;
- Developing objective criteria against which the controls adopted by responsible entities can be compared and measured in order to evaluate their adequacy, including subdividing the assets into different categories with different defined control objectives applicable to each subcategory;
- Defining with greater specificity the processes that responsible entities must have for Low Impact facilities under Reliability Standard CIP-003-5, Requirement R2; or
- Another equally efficient and effective solution.

Treatment of Lows Approach and Rationale

Approach

- Maintain a "single source" for Low Impact assets control requirements within CIP-003-5 Requirement R2 while leveraging existing requirements for establishing objective criteria:
  - CIP-004-5, CIP-005-5, CIP-006-5, and CIP-008-5
- Provide direction and clarity through supplemental guidance documentation

Rationale

The additions to R2, in particular the processes required under R2.2, are to address FERC Order 791 paragraphs 106-110 which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. The SDT has chosen to pull into R2 wording and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in the requirement. In Order 791 paragraphs 111-112, FERC was persuaded that creating and maintaining an inventory of Low Impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.

Challenges

Treatment of Lows
NEW CIP-003-5 R2, R2.1

R.2 Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3 (assets containing low impact BES Cyber Systems), shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

…

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

> **R.2.1** Review and obtain CIP Senior Manager approval at least once every 15 calendar months for a cyber security policy that addresses CIP-003-5, Requirement R2, Part 2.2.

(cont. next page)

Treatment of Lows
NEW CIP-003-5 R2.2, R2.2.1

R.2.2 Implement one or more documented processes that collectively address the following topics:

R.2.2.1 Operational or procedural control(s) that restrict physical access to the asset perimeter (Examples include fences, guards, site access policies, visitor policies, locked control houses, etc.)

Lists of authorized users are not required.

(cont. next page)

Treatment of Lows
NEW CIP-003-5 R2.2.2

R.2.2 Implement one or more documented processes that collectively address the following topics:

2.2.2 Access control(s) to restrict electronic access to low impact BES Cyber Systems via the asset's external routable protocol connections and Dial-up Connectivity, if any, such that:

2.2.2.1. All external routable protocol connections are protected via an identified access point that denies access by default and utilizes specific access permissions.

2.2.2.2 Where technically feasible, authentication is performed when establishing Dial-up Connectivity to a low impact BES Cyber System or network within the asset.

(cont. next page)

Treatment of Lows
NEW CIP-003-5 R2.2.3

R.2.2 Implement one or more documented processes that collectively address the following topics:

R.2.2.3 Cyber security incident response including conditions for activation of the response plan(s), roles and responsibilities of responders, and determination if an identified Cyber Security Incident is a Reportable Cyber Security Incident with notification of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law; and

(cont. next page)

Treatment of Lows
NEW CIP-003-5 R2.2.4

R.2.2 Implement one or more documented processes that collectively address the following topics:

> **R.2.2.4** Security awareness for the Responsible Entity's personnel that, at least once each calendar quarter, reinforces cyber security practices. At least once every 15 calendar months, the reinforcement should cover 2.2.1, 2.2.2, and 2.2.3 above.

Treatment of Lows
NEW CIP-003-5 Measures

M2. Examples of evidence may include, but are not limited to:

- One or more documented cyber security policies that addresses each of the areas in R2.2 and includes evidence of CIP Senior Manager review and approval at least every 15 months.
- One or more documented processes that addresses each of the areas in R2.2.
- For 2.2.1, documentation of the operational or procedural control(s).
- For 2.2.2, documentation of any external routable protocol connections, a list of access points for each connection, and evidence that each access point denies access by default and has specific access permissions.
- For 2.2.3, one or more documented cyber security incident response plans that includes the required parts.
- For 2.2.4, documentation that quarterly reinforcement of security awareness has been provided. Examples include dated copies of the information used as well as evidence of distribution method. Dated documentation of how the 2.2.1-2.2.3 areas were reinforced at least once every 15 calendar months.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Communication Networks

RELIABILITY | ACCOUNTABILITY




Communication Networks Discussion Items

- Reviewed NIST and ISO security controls referenced in FERC Order 791
- Identified the need for additional guidance around nonprogrammable components
- Identified potential compensating controls for protecting nonprogrammable components outside of the Physical Security Perimeter (PSP)
- Glossary definition of Communication Networks may not be needed to satisfy FERC concerns
- Ensured consistency with FERC Order 791 on Clarification/Rehearing regarding communication networks outside of the organization's control

Communication Networks Proposed Resolution

- New requirement Part 1.10 in CIP-006
  - Protects cabling and nonprogrammable components of an Electronic Security Perimeter (ESP) communication network located outside of a PSP
- Modified requirement Part 1.2 in CIP-007
  - More comprehensive coverage of physical ports
- No proposed definition for Communication Networks

Communication Networks
CIP-006 - New Part 1.10

1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components cannot be established, the Responsible Entity shall deploy and document alternative measures such as encrypting data that transits such cabling and components; or monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) or the alternative measures (e.g. data encryption or circuit monitoring).

Communication Networks
CIP-007 - Modified Part 1.2

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • PCA • nonprogrammable communication components located inside a PSP and inside an ESP Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA • nonprogrammable communication components located inside a PSP and inside an ESP	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable 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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Identify, Assess, and Correct

RELIABILITY | ACCOUNTABILITY




Identify, Assess, and Correct (IAC) Discussion Items

- Background on revision development
- Addressing zero defect and zero tolerance
- Proposed approach to add a requirement part to the appropriate IAC requirements
- RSAWs and associated compliance obligations will also play an important role
- The SDT is working with NERC staff on an FAQ document related to the Reliability Assurance Initiative (RAI)

Identify, Assess, and Correct (IAC) Proposed Resolution

- Zero defect / zero tolerance is an audit approach
- Removal of IAC language created a gap in performance
- Additional language for continuous improvement closes the gap
- Incorporation of NIST 800-53 concepts
  - Plan of action and milestones (PM-4)
  - Information Security Measures of Performance (PM-6)
  - Security Assessments (CA-2)
  - Assessment Procedure (CA-5)
  - Continuous Monitoring (CA-7)

Identify, Assess, and Correct (IAC) Proposed Resolution Example

- For CIP-007, a new R2.5
  - Review the process(es) associated with the implementation of security patch management for Parts 2.1, 2.2, 2.3, and 2.4 at least once every 15 calendar months and make updates as necessary.
- For CIP-007, update to R4.4
  - Review a summarization or sampling of logged events and alerts from Parts 4.1 and 4.2 as determined by the Responsible Entity at least once every 15 calendar days to identify undetected Cyber Security Incidents, process, system, or equipment failures. Develop an action plan to remediate or mitigate issues or process improvements identified in the reviews including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Transient Devices

RELIABILITY | ACCOUNTABILITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Transient Devices Discussion Items

- Requirements needed to address risks posed by transient devices
- Requirements should consider the following security elements:
  - Device authorization as it relates to users and locations
  - Software authorization
  - Security patch management and 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 (i.e. High, Medium, Low Impact).
- Leverage NIST SP 800-53 Maintenance and Media Protection security control families

Transient Devices Proposed Resolution

- Proposed new definitions
  - Transient Cyber Asset
  - Removable Media
- Proposed modified definitions
  - BES Cyber Asset
  - Protected Cyber Asset
- New requirement in CIP-010
- Additional guidance provided in CIP-004 and CIP-011

Transient Devices
CIP-010 – New Part 4.1

Part 4.1. Authorize Transient Cyber Assets and Removable Media 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. For Transient Cyber Assets, software, including but not limited to; OS or firmware where no independent OS exists, intentionally installed software; and

4.1.4. For Transient Cyber Assets, any security patches applied.

Transient Devices
CIP-010 – New Parts 4.2-4.5

Part 4.2. Deploy method(s) on Transient Cyber Assets to deter, detect, or prevent malicious code (per Transient Cyber Asset capability).

Part 4.3. Deploy method(s) for Removable Media to detect malicious code prior to each use (per device capability). Per Removable Media capability?

Part 4.4. For Transient Cyber Assets and Removable Media, mitigate the threat of detected malicious code.

Part 4.5 For those methods identified in Part 4.2 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

Transient Devices
CIP-010 – New Part 4.6

Part 4.6. Evaluate Transient Cyber Assets prior to initial use and at least once every 15 calendar months for modifications as documented in Part 4.1.3. For modification(s) identified in this section, take one of the following actions prior to use:

- Remediate by returning the Transient Cyber Asset to the baseline documented in Part 4.1.3; or
- Update the approved baseline in Part 4.1.3

Transient Devices
CIP-010 – New Part 4.7

Part 4.7. Evaluate Transient Cyber Assets prior to initial use and at least once every 15 calendar months for patches documented in Part 4.1.4 take one of the following actions prior to use:

- Apply the applicable patches; or
- 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 prior to use.

Transient Devices CIP-004 Guidance

- **Added to Requirement R2:**

  Additionally, training should address the risk when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135 Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems.

Transient Devices CIP-011 Guidance

- **Added to Requirement R1:**

  This includes information that may be stored on Transient Cyber Assets or Removable Media.

- **Added to Requirement R2:**

  If an applicable Cyber Asset, **Transient Cyber Asset, or Removable Media** is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Transient Devices Definitions

- **Transient Cyber Asset:** A Cyber Asset connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset for 30 consecutive calendar days or less, which is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
- **Removable Media:** Portable media 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.

Implementation Plan

- The proposed effective date (the date entities shall be compliant) for the Requirements.
- Identification of any new or modified definitions that are proposed for approval with the associated Reliability Standard.
- Whether there are any prerequisite actions that need to be accomplished before entities are held responsible for compliance with one or more of the Requirements.
- Whether approval of the proposed Reliability Standard will necessitate any conforming changes to any already approved Reliability Standards – and identification of those Reliability Standards and Requirements

Implementation Plan

- Each subgroup will be identifying the appropriate lead-time for any modifications

Standard	Requirement	Directive Addressed				Proposed Implementation Periods
		IAC	CN	TD	LI	
CIP–003–6	R2	X			X	Later of April 1, 2017 or [12] months following govt. approval.
	R4	X				Later of April 1, 2016 or [3] months following govt. approval.
CIP–004–6	R2	X				Later of April 1, 2016 or [3] months following govt. approval.
	R3	X				Later of April 1, 2016 or [3] months following govt. approval.
	R4	X				Later of April 1, 2016 or [3] months following govt. approval.
	R5	X				Later of April 1, 2016 or [3] months following govt. approval.
CIP–006–6	R1	X	X			For Parts 1.1 through 1.9, later of April 1, 2016 or [3] months following govt. approval. For new Part 1.10, later of April 1, 2016 or [12] following govt. approval.
	R2	X				Later of April 1, 2016 or [3] months following govt. approval.

Upcoming Schedule

March						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

April						
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

May						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

June						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

SDT Face-to-Face Meetings*	SDT Full-Team Conference Calls*	Identify, Assess, Correct*	Low Impact**
February 19-21 (9-5|8-5|8-12 ET)	March 3, 10, 24, 31 (2-4 ET)	March 4, 11, 25 (1-3 ET)	March 6, 13, 27 (1-3 ET)
March 18-20 (9-5|8-5|8-12 PT)	April 7, 14, 28 (2-4 ET)	April 1, 15, 29 (1-3 ET) 8 (3-5 ET)	April 3, 10, 17 (1-3 ET)
April 22-24 (9-5|8-5|8-12 ET)	May 5, 19, 28 (2-4 ET)	May 6, 20, 27 (1-3 ET)	May 1, 8, 22, 29 (1-3 ET)
May 12-14 (12-5|8-5|8-12 ET)	June 2 (2-4 ET)		

All calls will have the dial-in number of 1.866.740.1260 for ReadyTalk. For the meetings and calls above, *means the access code is 6515232. **means the access code is 1463851. All security codes are 247738 (CIPSDT). There will also be webinar capability for the events. Please go to www.ReadyTalk.com and insert the appropriate access code on the left side of the home page.

Communication Networks**	Transient Devices*
March 4 (11-1 ET) 11, 25 (3-5 ET)	March 6, 13, 27 (3-5 ET)
April 1, 9, 15, 29 (3-5 ET)	April 3, 10, 17 (3-5 ET)
May 6, 20, 27 (3-5 ET)	May 1, 8, 22, 29 (3-5 ET)

- Times subject to change based on extenuating circumstances
- ReadyTalk provided for all meetings and conference calls
- SDT reviewing the schedule this week and will likely make modifications – stay tuned!

Next Steps

- SDT in-person meetings scheduled:
  - May 12–14, 2014 (AEP-Columbus)
  - Registration and ReadyTalk information on the NERC calendar
- Post for 45-day first comment and ballot June 2–July 17, 2014:
  - SDT in-person meetings July and August, 2014 (will finalize at May meeting)
- Additional 45-day comment and ballot August 29-October 13, 2014 (if necessary)
- Final ballot October 31–November 10, 2014
- Presentation to the NERC Board of Trustees November 13, 2014
- File with applicable government authorities December 31, 2014

Resources

- This slide deck and other information relative to the CIP V5 Revisions SDT may be found on the Project 2014-02 Project Page under Related Files:
  - http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions-Related-Files.aspx
- Project plus list
  - Email Ryan Stewart or Marisa Hecht to join the list

Ryan.Stewart@nerc.net
202-644-8091

Marisa.Hecht@nerc.net
404-446-9620

Questions and Answers