

NERC-Led Technical Conferences

NERC's Headquarters – Atlanta, GA
Tuesday, January 21, 2014

Sheraton Phoenix Downtown – Phoenix, AZ
Thursday, January 23, 2014

RELIABILITY | ACCOUNTABILITY



- **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.

- Welcome & Safety Information
- Opening Remarks
- Standards Development Update
- Identify, Assess, and Correct
- Transition Study
- Communication Networks
- Low Impact Assets Protection
- Transient Devices
- Survey
- Closing

- Mark Lauby, Vice President and Director, Standards

- Engagement and discussion on considerations regarding the FERC Order No. 791 directives for the standard drafting team that is now being formed.
- Focus not on solution today but on industry input for the standard drafting team to use in finding a solution.

Standards Development Update

RELIABILITY | ACCOUNTABILITY



- January 15, 2014 – Standards Committee authorized Standard Authorization Request (SAR) for posting.
 - Scope of SAR
- January 17, 2014 – SAR posted for 30-day informal comment period.
- End of January – Standards Drafting Team appointed.

- <http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx>
- Components:
 - Standard Authorization Request

- January 21, 2014 – East Coast Technical Conference
- January 23, 2014 – West Coast Technical Conference
- Mid-February – Standard Drafting Team Kickoff
- May 5, 2014 – VRF Filing due
- August 4, 2014 – VSL Filing due
- February 3, 2015 – Modifications to IAC and physical protection of communication networks due
- February 3, 2015 – Informational Filing based on Survey due

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Identify, Assess, and Correct

RELIABILITY | ACCOUNTABILITY



- Enforcement and RAI Update
- Purpose of IAC Language
- FERC Support for Principles Underlying IAC
- FERC's Response
- FERC Order No. 791 Directive
- Changing Context
- Objective: Discuss removal or modification of IAC and integration of RAI

- Information and process flow improvements
- Pilots
 - Aggregation of minimal risk issues
 - Alternative path to enforcement (discretion)
- Timing
 - First cycle – October 2013 to April 2014

- Minimal risk issues only.
- Record maintained by registered entity during aggregation cycle.
- Format and content of record is similar to FFT spreadsheet.
- Periodic review of aggregated issues by Regional Entity.
 - First cycle began in October 2013; First evaluation of results will be in April 2014.
- Issues eligible for disposition through discretion.

- Minimal risk issues only.
- Notifications to NERC and FERC at the time of intake and disposition.
- Format and content of record is similar to FFT spreadsheet.
- Records available for review by NERC and FERC.

- Address “zero tolerance” compliance concerns regarding high frequency security obligations inherent to cybersecurity.
- Reduce administrative burden of compliance process.
- Incorporate lessons learned over the past four years.
- Promote development of strong internal controls.

- P 70: FERC stated that it supports:
 - NERC's move away from a zero tolerance approach to compliance.
 - The development of strong internal controls.
 - NERC's development of standards that focus on the activities that have the greatest impact to BPS reliability.

- PP 71-72: IAC language was unclear regarding:
 - Obligations imposed on responsible entities
 - Implementation by responsible entities; and
 - Enforcement.
- P 75: Concerned about compliance language included in standard.

- FERC directed NERC to remove or modify the “identify, assess, and correct” language.
 - P 67: Preferably, NERC should remove the “identify, assess, and correct” language.
 - P 67: Alternatively, NERC may propose equally efficient and effective modifications.
 - P 75: FERC would prefer approaches that would not involve the placement of compliance language within the text of Reliability Standards.
 - P 76: NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities.
- February 3, 2015 deadline for modifications.

- Removal of IAC language does not impact NERC's commitment to address "zero tolerance" concerns.
- However, RAI had not formally begun when the IAC language was initially introduced.
- P 73: The Reliability Assurance Initiative (RAI) process when fully developed may afford a consistent, informed approach that provides incentives for entities to develop robust internal control programs.
- Swift removal of IAC supports focus on transition activities while still addressing "zero tolerance" concerns.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Transition Study

RELIABILITY | ACCOUNTABILITY



- Purpose of V5 Transition Program
- CIP V5 Transition Program Elements
- Scope of Study
- Study Approach
- Key Themes & Lessons Learned

Purpose of the V5 Transition Program

Address V3 to V5
Transition issues.

Provide a clear
roadmap for V5
steady-state.

Justifies budget for
V5 implementation
and compliance.

Foster
communication and
knowledge sharing.

“Support all entities in the timely, effective, and efficient transition to CIP Version 5”

Periodic Guidance

- A new transition guidance will be provided after V5 Order

Implementation Study

- 6 entities with strong compliance cultures
- 6-8 month implementation of V5 for certain facilities
- Lessons learned throughout and after study phase

Compliance and Enforcement

- Integration with RAI
- Identify approaches to address IAC alternative processes

Outreach & Communications

- New website created for all Transition Program activity
- <http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx>


Training

- Quarterly training opportunities will be provided to industry
- V5 Technical Training will be provided at the March 4th CIPC Meeting in St. Louis

BES Cyber System Type	High	Medium
Control Centers	X	X
Backup Control Centers	X	X
Generation Dispatch Control Centers		X
Non-Routable Substations		X
Routable Substations		X
Generation facilities greater 1500 MW		X
Remote Access (Temporary)	X	X
Dedicated Remote Access	X	X
Data Centers	X	X

Determine Scope

Determine the scope of the Transition Study by selecting the Responsible Entities and their assets needed to provide a reasonable and sufficient sample of all entities who must comply with the NERC CIP Standards.



Conduct Studies

Conduct detailed studies with selected Responsible Entities to identify the challenges and issues associated with complying with NERC CIP Version 5.



Communicate Results

Communicate progress. Report conclusions and lessons-learned. Primary stakeholder audience is all Responsible Entities, not just Study Participants.

- Grouping BES Cyber Assets in Cyber Systems.
- 15 minute impact to operations.
- Approaches to defining PSP security controls around non-routable BES Cyber Systems.
- Remote access approaches.
- Approaches to address substation controls.
- Approaches to address generation controls.
- Configuration management of new BES Cyber Assets.
- What are the TFEable requirements? Approaches to minimize risk and administrative overhead.
- Alternatives to the IAC approach.



Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Communication Networks

RELIABILITY | ACCOUNTABILITY



- Definition of Cyber Asset and Communication Networks
- FERC's Response
- FERC Order No. 791 Directive
- Communication Networks definition
- New or Modified Reliability Standard
- Objective: Gather industry input on the potential scope covered in communication networks definition and requirements

- Inclusion of communication networks in the Cyber Asset definition was removed in version 5.
- Cyber Asset Definition:
 - Programmable electronic devices ~~and communication networks~~, including the hardware, software, and data in those devices.
- Many components of communication networks cannot strictly comply with the version 5 standards.

- P 148: FERC was persuaded that communication networks are not necessary in the Cyber Asset definition.
- P 149: However, “[W]e remain concerned that a gap in protection may exist, as the CIP version 5 Standards do not address security controls needed to protect the nonprogrammable components of communications networks.”

- P 150: FERC directed NERC to:
 - create a definition of communication networks; and
 - develop new or modified Reliability Standards that address the protection of communication networks to be filed for approval by February 3, 2015.
- P 150: FERC directed FERC staff to include the issue of protecting nonprogrammable components of communication networks in the FERC staff-led technical conference.

- P 150: FERC Statements on Responding to Directives:
 - The definition of communication networks should include what equipment and components should be protected.
 - The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks.

- Recognizing that the definition of communication networks needs a defined scope, what are some considerations for identifying the scope of a communication network?
 - Examples: Current ESP networks and communications between ESPs; vendor connections; point-to-point networks, etc.

- What considerations should the standard drafting team address when weighing the following options:
 - Modify CIP V5 standards to address communication networks; or
 - Develop a new standard for communication networks?

Lunch

Resume at 1:00 p.m. MT

RELIABILITY | ACCOUNTABILITY



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Low Impact Assets Protection

RELIABILITY | ACCOUNTABILITY



- CIP-003-5 Requirement R2
- FERC's Response
- FERC Order No. 791 Directive
- FERC Order No. 791 Alternatives
- Examples of Approaches
- Objective: Discussion on considerations of options to meet the directive

- **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.

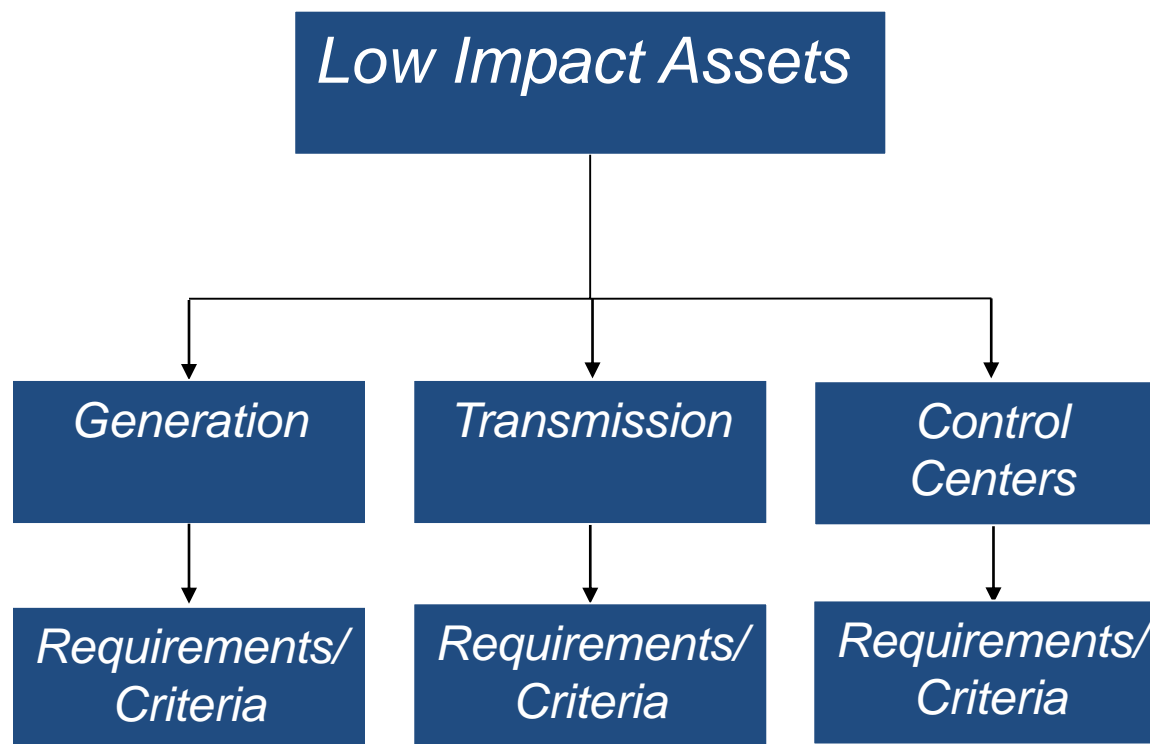
- P 107: Standards do not:
 - Require specific controls for Low Impact assets; nor
 - Contain clear, objective criteria from which to judge sufficiency of the controls ultimately adopted by responsible entities for Low Impact assets.
- P 108: Absence of objective criteria to evaluate controls chosen by responsible entities:
 - Introduces an unacceptable level of ambiguity,
 - Brings potential inconsistency into compliance process, and
 - Creates unnecessary gap in reliability.

- P 108: FERC directed NERC to develop modifications that address its concerns for Low Impact assets.
- P 106: “[W]hile we do not require NERC to develop specific controls for Low Impact facilities, we do require NERC 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.”

- P 108: FERC suggested the following alternatives to address the directive:
 1. Require specific controls for Low Impact assets, including subdividing the assets into different categories with different defined controls applicable to each subcategory; or
 2. Develop 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; or
 3. Define with greater specificity the processes that responsible entities must have for Low Impact facilities under CIP-003-5, Requirement R2; or
 4. Develop another equally efficient and effective solution.

- Include Low Impact assets in the matrices of other CIP standards that address cyber security awareness, physical security controls, etc.
- Include requirement parts from the matrices in CIP-003, Requirement R2 scaled to protect Low Impact assets.
- Include policy objectives in CIP-003, Requirement R2 that ensure intent is clear.

- Example of Low Impact Assets subcategories:



- What are important issues for the standard drafting team to consider in finding a solution?
- We will keep within these four technical areas:
 - Cyber security awareness;
 - Physical security controls;
 - Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
 - Incident response to a Cyber Security Incident.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Transient Devices

RELIABILITY | ACCOUNTABILITY



- Definition of BES Cyber Asset
- FERC's Response
- FERC Order No. 791 Directive
- Objective: Discussion on considerations of options to meet the directive

- NERC's proposed definition of BES Cyber Asset, in part, stated a Cyber Asset is not a BES Cyber Asset if:
 - For 30 consecutive calendar days or less:
 - It is directly connected to:
 - A network within an ESP; or
 - A Cyber Asset within an ESP; or
 - A BES Cyber Asset.
 - AND it is used for:
 - Data transfer; or
 - Vulnerability assessment; or
 - Maintenance; or
 - Troubleshooting purposes.

- P 132: Although recognizing treating all transient devices as BES Cyber Assets is unduly burdensome, FERC is concerned that CIP Version 5 Standards do not provide adequately robust protection from the risks posed by transient devices.

- P 132: FERC directed NERC to develop either new or modified standards to address the reliability risks posed by connecting transient electronic devices (*e.g.*, thumb drives and laptop computers) to BES Cyber Assets and Systems.

- P 136: FERC expects NERC to consider the following:
 - Device authorization as it relates to users and locations
 - Software authorization
 - Security patch management
 - Malware protection
 - Detection controls for unauthorized physical access
 - Processes and procedures for connecting transient devices to systems at different security classification levels.

- Objective: What are considerations regarding options to address the reliability risks posed by connecting transient electronic devices to BES Cyber Assets and Systems?
 - Example approaches: separate standard, separate requirements, applicable systems column

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Survey

RELIABILITY | ACCOUNTABILITY



- Definition of BES Cyber Asset
- FERC's Response
- FERC Order No. 791 Directive
- Objective: Discuss appropriate questions for survey

- BES Cyber Asset definition
 - Includes Cyber Assets that *“if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment....”*
- The “15-minute” parameter

- P 123: BES Cyber Asset identification is critical in applying CIP Version 5 Standards.
- P 123: Better understanding of the scope of assets included as a result of the 15-minute parameter is key.

- P 124: FERC directed NERC to conduct a survey of Responsible Entities during the CIP Version 5 Standards implementation periods to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the “15-minute” parameter specified in the definition.

- PP 124-25: By February 3, 2015, NERC must submit an informational filing that explains:
 - Specific ways in which entities determine which Cyber Assets meet the 15-minute parameter.
 - Types or functions of Cyber Assets that are excluded and why.
 - Common problem areas of improperly designating BES Cyber Assets.
 - Feedback from each Regional Entity participating in the CIP Implementation Study.

- How would you phrase the survey questions in order to meet FERC's directive?

- Thank you!
- Next Steps
- Getting added to the “Plus List”
- Outreach activities



Questions and Answers