

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

# Project 2019-02

## BES Cyber System Information Access Management

Industry Webinar  
January 16, 2020

RELIABILITY | RESILIENCE | SECURITY



- Presenters
  - SDT
    - Chair, John Hansen, Exelon
    - Vice Chair, Josh Powers, SPP
    - Member, Conor Martin, Arizona Public Service
    - Member, William Vesely, Consolidated Edison Company of New York, Inc.
  - NERC Staff
    - Latrice Harkness,
- Administrative Items
- Proposed Revisions
- Implementation Plan
- Next Steps
- Questions and Answers

- 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. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

- **Public Announcement**
  - Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.
- **Presentation Material**
  - Information used herein is used for presentation purposes and may not reflect the actual work of the official posted materials
- **For the official record**
  - This presentation is not a part of the official project record
  - Comments must be submitted during the formal posting

Name	Organization/ Company
John Hansen (Chair)	Exelon
Josh Powers (Vice Chair)	Southwest Power Pool, Inc. (SPP)
Victoria Bethley	Duke Energy
Andrew Camargo	San Diego Gas & Electric
Sharon Koller	American Transmission Company, LLC
Michael Lewis	Southern California Edison
Conor Martin	Arizona Public Service
Yoel Piney	PSEG
Regan Plain	Minnkota Power Cooperative
Joshua Roper	Westar and KCP&L, Eversource Companies
Clay Walker	Cleco Corporate Holdings LLC
William Vesely	Consolidated Edison Company of New York, Inc.

Name	Organization/ Company
Latrice Harkness – Standards	North American Electric Reliability Corporation
Marisa Hecht – Legal	North American Electric Reliability Corporation
Lauren Perotti – Legal	North American Electric Reliability Corporation

- CIP-011-2, Requirement 1
  - Focused on protecting locations of BCSI
- CIP-011-3, Requirements 1 and 2 (new)
  - Focused on protecting BCSI regardless of location (information-centric)
  - Changed Applicable Systems column to Applicability column

- Entirely new requirement (CIP-011-3, Requirement R2)
- Layer of defense against bad actors who may physically or electronically obtain BCSI but not use or modify BCSI
- Requires entities to develop a key management program
- Part 2.1
  - Develop key management process(es), where applicable
  - Includes key management life cycle in requirement for clarify and enforceability (life cycle phases based on NIST 800-130)
- Part 2.2
  - Implement controls around key management separation of duties
  - Enforces separation of duties between the custodial entity and the key owner



- New sub-requirement (CIP-011-3, Requirement R1, Part 1.4)
- Risk-based approach to address security objectives
- Requires entities to implement a BCSI risk management methodology
- Requirement R1, Part 1.4.1
  - Perform an initial risk assessments of any vendor(s) selected to store BCSI
- Requirement R1, Part 1.4.2
  - Perform risk assessments of any vendor(s) storing BCSI every 15 calendar months
- Requirement R1, Part 1.4.3
  - Document results of risk assessments performed in Parts 1.4.1 and 1.4.2 and an action plan to remediate or mitigate identified risks

- Moved requirements from CIP-004, Requirements R4 and R5, to CIP-011, Requirement R1
- CIP-004, Requirement R4, Part 4.1.3
  - New CIP-011, Requirement R1, Part 1.3
  - Authorization of access to BCSI
- CIP-004, Requirement R4, Part 4.4
  - New CIP-011, Requirement R1, Part 1.6
  - Review of access to BCSI every 15 calendar months
- CIP-004, Requirement R5, Part 5.3
  - New CIP-011, Requirement R1, Part 1.5
  - Termination of access to BCSI within 24 hours

- CIP-011-2, Requirement R2, now becomes Requirement R3
- Consolidated BES Cyber Asset reuse and disposal into one requirement (now Requirement R3, Part 3.1)
- Expanded applicability of sanitization and destruction of data storage media on BES Cyber Assets beyond BCSI
- Did not exclude External Routable Connectivity
- Included PCA as applicable for CIP-011, Requirements R1 and R2

- 18-month Implementation Plan
- The 18-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking the following steps:
  - Establish and/or modify vendor relationships to establish compliance with the revised CIP-011-3 Requirements
  - Address the increased scope of the CIP-011-3 “Applicable Systems” and “Applicability” column, which has a focus on BES Cyber System Information as well as the addition of Protected Cyber Assets (PCA)
  - Develop additional sanitization programs for the life cycle of BES Cyber Systems, if necessary

- Comment period
  - [Project 2019-02 page](#)
  - 45 Days – December 20 – February 3, 2020
  - Ballot – January 24, 2019 – February 3, 2020
- SDT Meeting
  - February 25-27, 2020
  - Respond to Comments
- Point of contact
  - Latrice Harkness, Senior Standards Developer
  - [Latrice.Harkness@nerc.net](mailto:Latrice.Harkness@nerc.net) or call 404-446-9728
- Webinar posting
  - 48-72 hours
  - Standards Bulletin

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record



# Questions and Answers