NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2020-03 Supply Chain Low Impact Revisions

Industry Webinar
September 9, 2021

RELIABILITY | RESILIENCE | SECURITY




Agenda

Administrative

- Review NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

- Standard Drafting Team (SDT)
- Supply Chain Report
- Standard Updates
- Next Steps
- FAQs
- Questions and Answers

NERC Antitrust

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.

NERC Public Disclaimer

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.

Project 2020-03 SDT

Name	Organization/ Company
Tony Hall (Chair)	LG&E and KU Energy
Kevin Conway (Vice Chair)	Pend Oreille County Public Utility District No. 1
Steven Briggs	Tennessee Valley Authority
Shannon Ferdinand	Capital Power
Joseph Gatten	Xcel Energy
John Grube	Duke Energy – Midwest Regional Services
Barry Jones	WAPA
Roy Kiser	Southern Company
Ida Mauricio	CPS Energy
Karl Perman	CIP Corps
Harold Sherrill	RWE Renewables Americas
Jeffrey Sweet	AEP

Supply Chain Report

- Supply Chain report/NERC Board of Trustees data request/Final report
  - *Supply Chain Risk Assessment* published in December 2019 recommended modification to include low impact BES Cyber Systems with remote connectivity be included in supply chain risks
- Proposed Modifications to CIP-003
  - BES Cyber Systems that allow vendor remote access:
    - Detect known or suspected malicious communications for both inbound and outbound communications
    - Determine when active vendor remote access sessions are initiated
    - Disable active vendor remote access sessions when necessary

Requirement 1.2. Changes

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; ~~and~~

1.2.6. Vendor remote access; and

~~1.2.6.~~1.2.7. Declaring and responding to CIP Exceptional Circumstances.

Attachment 1 changes – Adding Section 6

- **Section 6**: Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:
  - **6.1** Having one or more method(s) for determining vendor remote access sessions;
  - **6.2** Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and
  - **6.3** Having one or more method(s) for disabling vendor remote access.

Posting

- CIP-003-X
  - Clean and redline
  - -X version to not overlap with virtualization, changes will be incorporated after final ballot
- Implementation Plan
- Technical Rationale
- Posting Date: August 27-October 11, 2021
- Project Page

Next Steps

- Respond to Comments
  - Team Meeting in October 2021
  - Projected Second Posting in December 2021/January 2022
- Point of Contact
  - Alison Oswald, Senior Standards Developer
    - Alison.oswald@nerc.net or call 404-446-9668
- Webinar Slides and Recording Posting
  - Within 48-72 hours of Webinar completion
  - Will be available in the Standards, Compliance, and Enforcement Bulletin

FAQ

- Why did the SDT add a Section 6 to the Attachment 1 criteria rather than address electronic and remote access in the existing Section 3?
- Why did the SDT use the term “determine” vendor remote access?
- Did the SDT intentionally use the term “interactive remote access” instead of “Interactive Remote Access” (the defined term)?

Questions and Answers Objectives

- Informal Discussion
  - Via the Questions and Answers Objectives 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 regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the SDT

Questions and Answers

Webinar has ended – Thank You