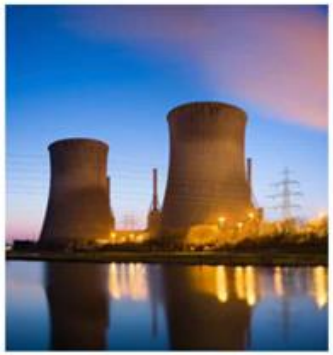
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2020-03 Supply Chain Low Impact Revisions

Industry Webinar
March 16, 2022

RELIABILITY | RESILIENCE | SECURITY

Agenda

Administrative

- Review NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

- Standard Updates
- Technical Rationale
- Implementation Plan

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.

Attachment 1 changes – Section 6

Section 6. Electronic Vendor Remote Access Security Controls: 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 electronic vendor remote access. These processes shall include:

6.1 One or more method(s) for determining electronic vendor remote access where such access has been established under Section 3;

6.2 One or more method(s) for disabling electronic vendor remote access where such access has been established under Section 3; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.

6.1 One or more method(s) for determining electronic vendor remote access where such access has been established under Section 3;

Technical Rationale

The objective of Attachment 1 Section 6.1 is for entities to have visibility of electronic vendor remote access on their low impact BES Cyber Systems. Such visibility increases an entity's ability to detect, respond and resolve issues that may originate with or be tied to a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have a method to determine electronic vendor remote access.

6.2 One or more method(s) for disabling electronic vendor remote access where such access has been established under Section 3; and

Technical Rationale

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable electronic vendor remote access in the event of a security event, the inability of a responsible entity to terminate a connection may allow malicious or otherwise inappropriate communication to propagate, contributing to a degradation of a BES Cyber Asset's function. Enhanced visibility into electronic vendor remote access and the ability to terminate electronic vendor remote access could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable electronic vendor remote access.

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.

Technical Rationale

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications by vendors, such that the entity may respond to and remediate resulting impacts. This sub part is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with low impact BES Cyber Systems.

Implementation Plan

- Draft 1:
  - 18 months for all of Attachment 1 Section 6

- Draft 2:
  - Drafting team is currently proposing a phased approach
  - Attachment 1 Section 6 Part 6.1 and 6.2 - 18 months
  - Attachment 1 Section 6 Part 6.3 - 6 additional months (24 months from approval)

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: February 25 – April 15, 2022 (extended)
- Project Page

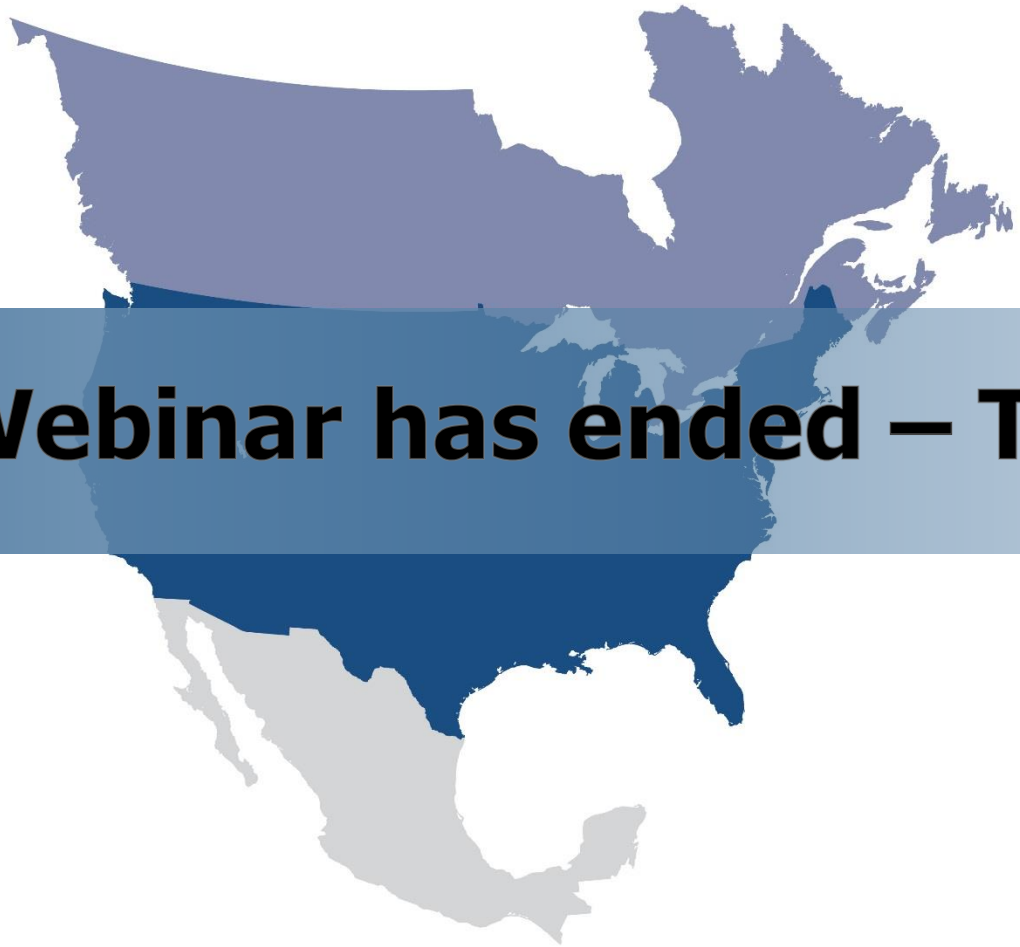
Next Steps

- Respond to Comments
  - Team Meeting in April 2022
  - Discuss next steps
- 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

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