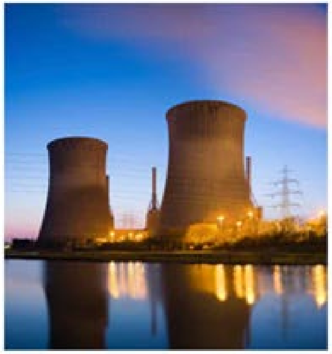
NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2020-03 Supply Chain Low Impact Revisions

Industry Webinar
July 27, 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.

Slido

Or

www.Slido.com

Event Code: 3386941

Password: 2020-03

Overview

- Defined terms and why we did not use them (IRA and system to system)
  - Consistency with CIP-005 R2
- Reordered “vendor electronic”
- Clarifying changes to TR
- Attachment 2 is not all inclusive list
- Addressing recommendations from NERC board resolution based on the supply chain report
- IP extended

Attachment 1 changes – Section 6

Section 6.~~-Electronic~~ Vendor Electronic 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 electronic remote access, where such access has been established under Section 3.1. These processes shall include:

- **6.1** One or more method(s) for determining ~~electronic~~ vendor electronic remote access ~~where such access has been established under Section 3~~;
- **6.2** One or more method(s) for disabling ~~electronic~~ vendor electronic remote access~~ where such access has been established under Section 3~~ ; and
- **6.3** One or more method(s) for detecting known or suspected inbound and outbound malicious communications. ~~for both inbound and outbound vendor communications.~~

Technical Rationale

Terminology addressed in the updated Technical Rationale

- Remote (access)
- Vendor
- Malicious Communications
- Active and Read-Only

Technical Rationale

- Remote (access)

  - Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) that matches existing electronic remote access in other CIP standards.

  - Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low-impact assets and systems

Technical Rationale

- Vendor
  - CIP-013 on Vendor meaning (footnote from Draft 1 of this project was removed in error)
    - The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Technical Rationale

- Malicious Communication
    - ○ Why applicable to Low Impact BCS and not Medium (excluding at Control Centers)?
    - ○ More robust security controls are applicable to Medium Impact BES Cyber Systems Controls that prevent a vendor’s direct access to those systems (e.g. multi-factor authentication, Intermediate Systems)
    - ○ Vendors tend to be more involved with the operation of many Low Impact generation sites such as wind farms
    - ○ Requirement has scope limited to just vendors access Low Impact BES Cyber Systems remotely – No obligation for internal communications
    - ○ In line with the NERC stated risk-based model

Technical Rationale

- Active and Read-only

- Refrained using these terms due to potential unintended consequences that could include but are not limited:
  - Increased compliance activities and compliance risk
  - Increasing the scope of the SAR
  - Restriction in the application of the risk-based model

Implementation Plan

- Previous drafts had staggered implementation timelines
- Drafting team is currently proposing 36 months for all requirements based on industry comments:
  - Variability in entity size and number of assets that need to be reviewed
  - Potential to have to plan for multiple outages of assets
  - Supply chain challenges
  - Development and approval of budgets

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: July 6 – August 19, 2022
- Project Page

Next Steps

- Respond to Comments
  - Team Meeting in August 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 Slido
  - Not using Chat or Q&A in WebEx
  - 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

Or

www.Slido.com

Event Code: 3386941

Password: 2020-03

Webinar has ended – Thank You