NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2019-03 Cyber Security Supply Chain Risk Management

May 14, 2020
11:00 a.m. – 12:30 p.m. Eastern

RELIABILITY | RESILIENCE | SECURITY




Agenda

Administrative

- Review NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

- Project Status
- Standards Updates
- Next Steps
- 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.

Timeline Project 2019-03

- FERC Order 850 issued October 18, 2018
  - Directed inclusion of EACMS
- NERC Cyber Security Supply Chain Risks Report published May 17, 2019
  - Recommended inclusion of PACS
- SDT Team held second meeting March 23-26, 2019
- This is the second formal posting
  - 45-day comment period, May 7 – June 22, 2020
  - 10-day ballot period, June 12 – June 22, 2020

Standards Updates

- Goal is to make minimal changes to meet the FERC Order 850 and the NERC Supply Chain report
  - Changes include adding EACMS and PACS to CIP-005, CIP-010, and CIP-013
- Coordinating with ongoing CIP projects
  - 2016-02 – Modifications to CIP Standards
  - 2019-02 – BES Cyber System Information Access Management

Draft CIP-005-7

CIP-005-6 Language (Removed)	CIP-005-7 Language (Proposed)
Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.1: Have one or more methods for ~~determining~~ detecting ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.
Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.2: Have one or more method(s) to ~~disable~~ terminate established ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.

Draft CIP-005-7

- Interactive Remote Access (IRA)
  - User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol.
  - Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP).
  - Remote access may be initiated from:
    - Cyber Assets used or owned by the Responsible Entity,
    - Cyber Assets used or owned by employees, and
    - Cyber Assets used or owned by vendors, contractors, or consultants.
  - Interactive remote access does not include system-to-system process
- Remote Access to EACMS
  - EACMS used for remote access to EACMS

Draft CIP-010-4

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

Draft CIP-013-2

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated (i) ~~Interactive R~~remote A~~a~~ccess, and (ii) system-to-system remote ~~access with a vendor(s)~~.

Posting

- Draft 2 of CIP-005-7, CIP-010-4 and CIP-013-2
  - Clean and redline to last posted versions
- CIP-005-7 Summary of Changes
  - Comparison of CIP-005-6 Requirement R2.3 and R2.4 language against CIP-005-7 Requirement R3 language
- Implementation Plan
  - Modified from 12 to 18 months based on industry feedback
- Updated VRF/VSL Justification
  - VSL's updated in CIP-005-7 due to new Requirement R3
- Technical Rational for all three standards
- Draft Implementation Guidance for all three standards
  - Pending ERO approval

Next Steps

- Additional Ballot and Comment Period
  - May 7 – June 22, 2020
  - Project 2019-03 Project Page
- Respond to Comments
  - Team Meeting in July
  - Projected Third Posting in July/August
- Point of Contact
  - Alison Oswald, Senior Standards Developer
  - Alison.oswald@nerc.net or call 404-446-9668
- Webinar Posting
  - 48-72 hours
  - Standards Bulletin

Q & A Objectives

- 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 regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the Standard Drafting Team

Questions and Answers

Webinar has ended – Thank You