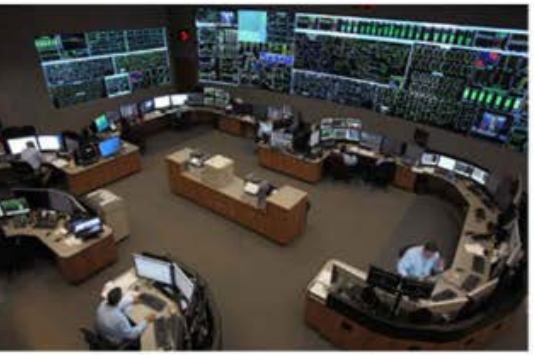
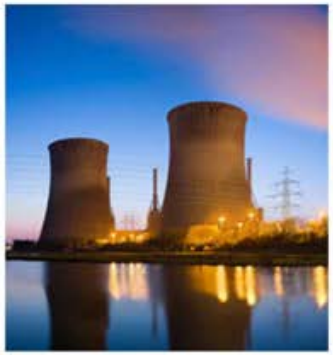
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Project 2019-03 Cyber Security Supply Chain Risks

August 5, 2020
1:00 – 2:30 p.m. Eastern

RELIABILITY | RESILIENCE | SECURITY

# Agenda

- Review NERC Antitrust Compliance Guidelines and Public Announcement
- Project Status
- Standards Updates
- Next Steps
- Questions and Answers (Q & A)

# 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
  - FERC Directed Deadline December 26, 2020
- NERC Cyber Security Supply Chain Risks Report published May 17, 2019
  - Recommended inclusion of PACS
- SDT Team held a third meeting June 30 – July 2, 2020
- This is the third formal posting
  - 45-day comment period, July 28 – September 10, 2020
  - 10-day ballot period, September 1 – September 10, 2020

# Standards Updates

- Goal is to make required 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, collectively referred to as the Supply Chain Cyber Security Risks Management standards
- Coordinating with ongoing CIP projects
  - 2016-02 – Modifications to CIP Standards
  - 2019-02 – BES Cyber System Information Access Management

# Draft CIP-005-7 (v3)

**R3.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

**M3.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

# Draft CIP-005-7 (v3)

| CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| **3.1** | EACMS and PACS associated with High Impact BES Cyber Systems ~~and their associated:~~ ~~EACMS;~~ ~~PACS; and~~ ~~PCA~~ EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity ~~and their associated:~~ ~~EAMCS;~~ ~~PACS; and~~ ~~PCA~~ | Have one or more method(s) ~~for detecting~~ to determine authenticated vendor-initiated remote connections ~~access sessions~~. | Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated ~~active~~ vendor-initiated remote ~~access~~ connections,~~(including system to system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions),~~ such as:<br>• Methods for accessing logged or monitoring information to ~~determine active~~ determine authenticated vendor-initiated remote connections~~access sessions.;~~<br>• ~~Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or~~<br>~~Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.~~ |

# Draft CIP-005-7 (v3)

| CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| **3.2** | EACMS and PACS associated with High Impact BES Cyber Systems ~~and their associated: EACMS; PACS; and PCA~~<br>EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity ~~and their associated: EACMS; PACS; and PCA~~ | Have one or more method(s) to terminate ~~established~~ authenticated vendor-initiated remote ~~access~~ connections ~~sessions~~ and control the ability to reconnect. | Examples of evidence may include, but are not limited to, documentation of the methods(s) used to ~~disable~~ terminate ~~active~~authenticated vendor-initiated remote ~~access~~ connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.<br>~~(including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions), such as:~~<br>~~PCA or BES Cyber System Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~<br>• ~~PCA or BES Cyber System Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~<br>• ~~PACS or EACMS Methods to disable active vendor remote access either through Electronic Access Point, an Intermediate System or any other method of remote access~~ |

# Draft CIP-010-4 (v3)

| CIP-010-~~3~~4 Table R1 – Configuration Change Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.6 | High Impact BES Cyber Systems and their associated:<br>1. EACMS; and<br>~~1.~~2. PACS<br><br>Medium Impact BES Cyber Systems and their associated:<br>1. EACMS; and<br>~~1.~~2. PACS<br><br>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:<br><br>1.6.1. Verify the identity of the software source; and<br><br>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 (v3)

**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 vendor-initiated ~~(i)~~ remote access~~, and (ii) system-to-system remote access.~~.

# Summary

- Summary of changes from draft two (2) to draft three (3)
  - CIP-005-7
    - Recursive requirements (Hall of mirrors)
    - Restored Requirement R2 Part 2.4 and 2.5 to previous approved language
    - New Requirement R3 for inclusion of EACMS and PACS
  - CIP-010
    - No changes
  - CIP-013
    - Minor change to 1.2.6.

# Posting

- Draft 3 of CIP-005-7, CIP-010-4 and CIP-013-2
  - Clean and redline (last approved and last posted)
  - CIP-005-7 Summary of Changes
- Implementation Plan
- Updated VRF/VSL Justification
- Technical Rational for all three standards
- Draft Implementation Guidance for all three standards
  - Pending ERO approval

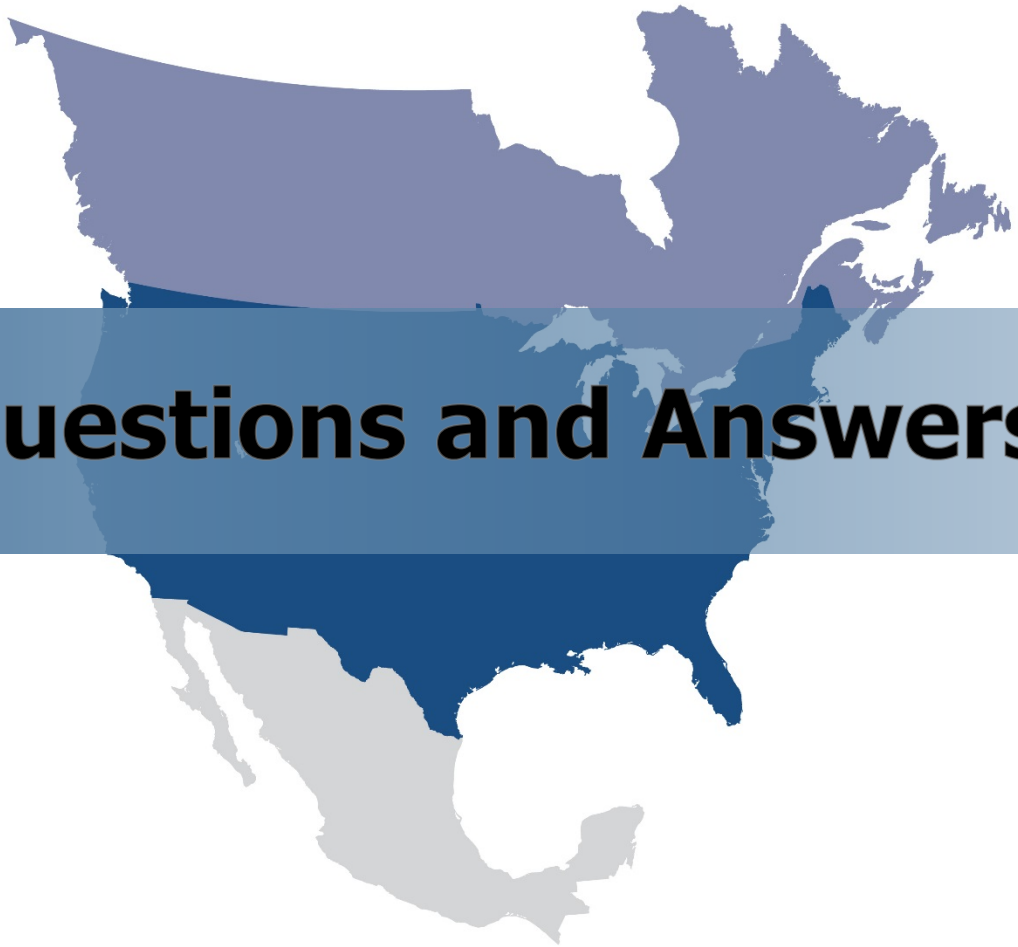
# Next Steps

- Additional Ballot and Comment Period
  - July 28 – September 10, 2020
  - Project Page: https://www.nerc.com/pa/Stand/Pages/Project2019-03CyberSecuritySupplyChain-Risks.aspx
- Point of Contact
  - Jordan Mallory, Senior Standards Developer
    - Jordan.Mallory@nerc.net or 404-446-2589
  - Alison Oswald, Senior Standards Developer
    - Alison.oswald@nerc.net or call 404-446-9668
- Webinar Posting
  - 48-72 hours
  - Standards Bulletin

# Q & A Objectives

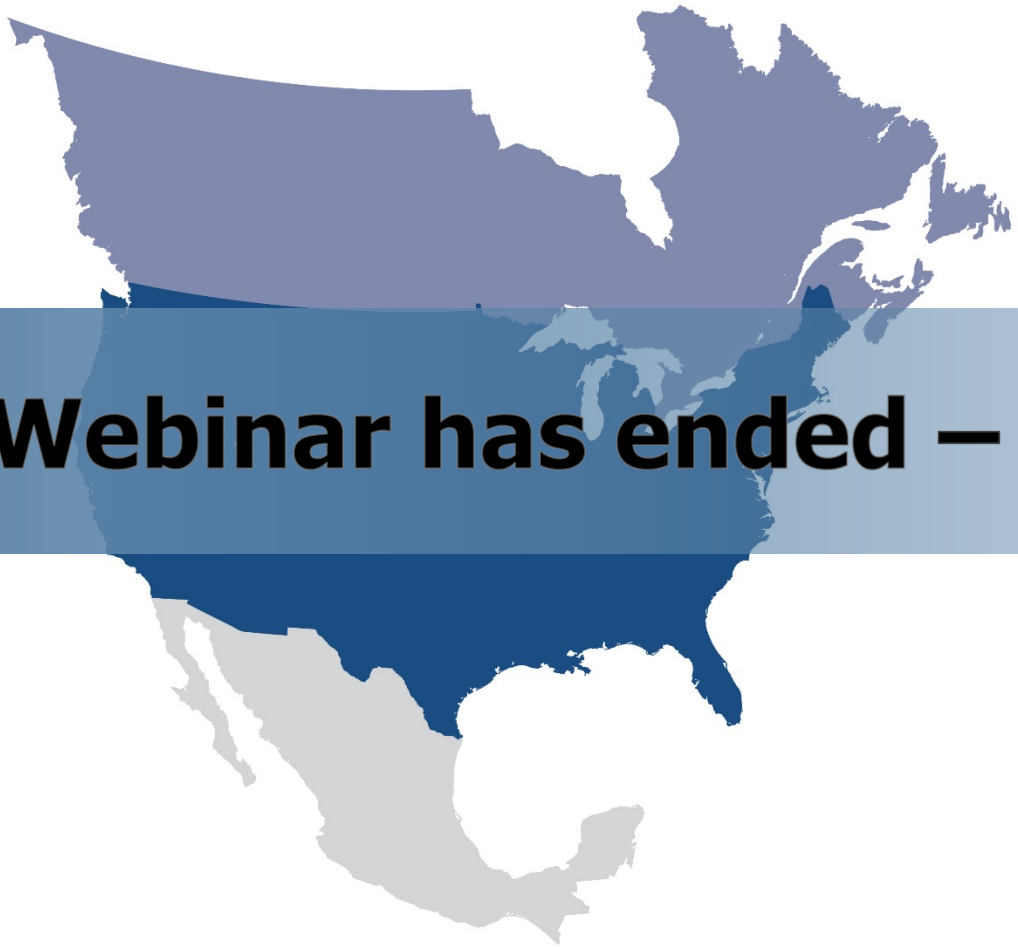
- Informal Discussion
  - Via the Q & A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



# Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



# Webinar has ended – Thank You