NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2023-04 Modifications to CIP-003

September 27, 2024

RELIABILITY | RESILIENCE | SECURITY




Administrative Items

- NERC Antitrust Guidelines
  - 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.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Agenda

- Background
- Additional Draft Comments
- Revisions to CIP-003-11
- Implementation Plan
- Q&A

Drafting Team (DT) Members

	Name	Entity
Chair	Tony Hall	LG&E and KU
Vice Chair	Jay Cribb	Southern Company
Members	Monica Jain	Southern California Edison
	Clayton Whitacre	Great River Energy
	Barry Jones	Western Area Power Administration
	Robert Montgomery	Duke Energy
	Peggy McDannald	Associated Electric Cooperative, Inc.
	Josef Chesney	Powder River Energy Corp
	Sean Randles	Intersect Power
	Lemon Williams	Pine Gate Renewables
	Jeff Sykes	Utility Services

LICRT Report Recommendations

- LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems
- LICRT Report
- CIP Standard Revisions
  - Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
  - Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
  - Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.
- Project 2023-04 SAR includes the LICRT recommendations

Previous Ballot Results

- Standard – 80.58%
- Implementation Plan (IP) – 64.01%

Due to the IP not passing, both CIP-003-11 and IP are being posted again

Recent Draft Comment Themes

- The alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once.
  - Attachment 1 Section 3.1.2
- Combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version.
- Changes to Attachment 1 header for multi-impact SCI/BCS
  - Clarifying High/medium process for low impact SCI

CIP-003-11

- Two Drafting Teams modifying CIP-003-9 during previous ballots
  - Project 2016-02 (Virtualization) posted CIP-003-10 (Board approved in May)
  - Project 2023-04 (LICRT) posted CIP-003-A
- Project 2023-04 has changed from version “–A” to “-11”
- CIP-003-11 is an overlay of 2023-04 changes on top of the Board approved -10 version.

CIP-003-11 Revisions

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 ~~or~~and for SCI that supports a low impact BCS, if any, where electronic access is:

Technical Rationale

- Decrypting communications for detection
- Multiple ways to authenticate individual users
- Conforming changes

Implementation Plan

- CIP-003-11 Implementation Plan
  - Three (3) years from regulatory approval to be compliant with CIP-003-11
  - Attachment 1 Section 3.1.2 until ***the later of***: (1) April 1, 2029; or (2) the effective date of Reliability Standard CIP-003-11
  - General considerations:
    - Revise cyber security policies, plans, and procedures.
    - Hire and train new staff to implement the new cyber security controls.
    - Reconfigure system, network, or security architectures.
    - Purchase, procure, and install new technologies.
    - The effective date of CIP-003-9 is April 1, 2026.
    - The requested effective date of CIP-003-10 is the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority

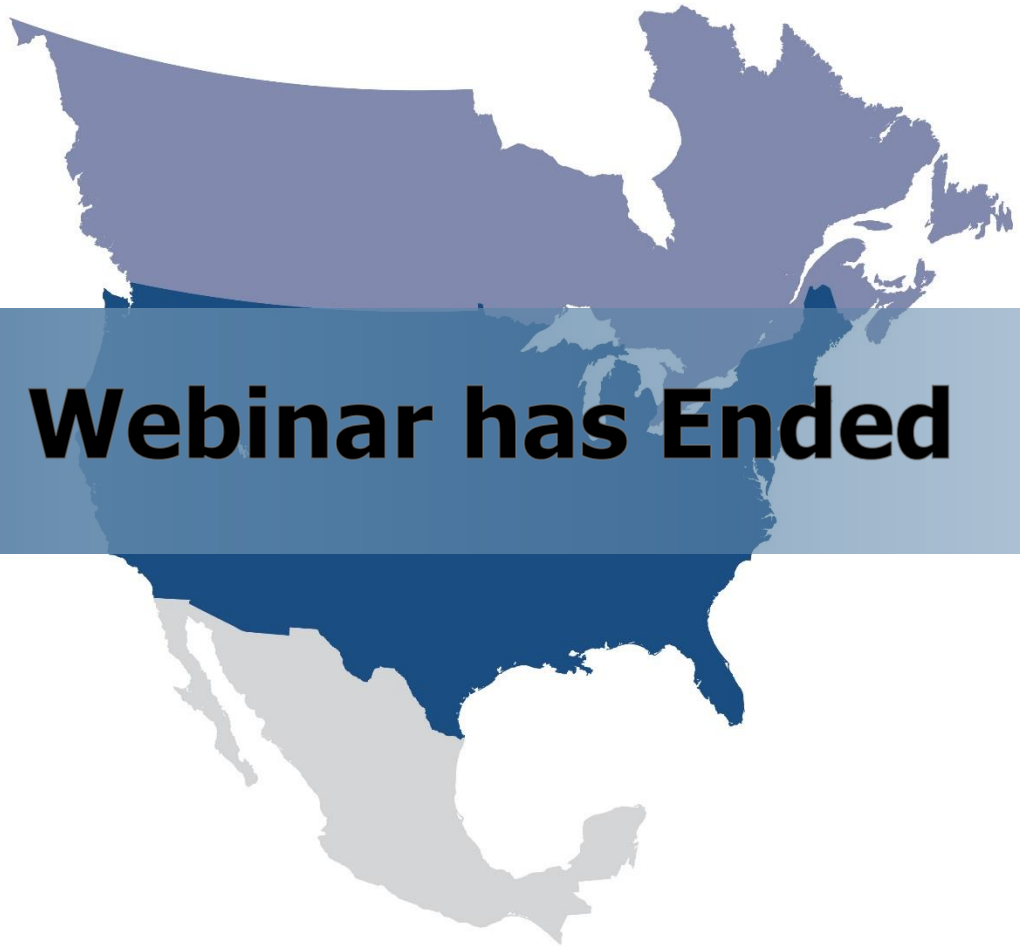
Next Steps

- CIP-003-11 Posting
  - Comment open September 11 - October 10, 2024
  - Ballot open October 1 – 10, 2024
- Respond to Comments
  - Team Meetings in October 2024
  - Target Final Ballot in November 2024
  - Present to NERC Board in December 2024
- Point of Contact
  - Alison Oswald, Manager of Standards Development
    - Alison.Oswald@nerc.net or call 404-275-9410
- 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