NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2023-04 Modifications to CIP-003

June 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
- CIP-003-12
- 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

Recent Draft Comment Themes

- Additional Ballot:
  - January 30 – March 14, 2024
  - 60.34% approval
- Section 3.1.3,'s recommendation of changing "when" to "prior to" in order to clarify that the remote user be authenticated prior to access, as explained in the Technical Rationale.
- Clear language in the implementation guidance describing the change from use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, Part 3.1, i-iii.
- The costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements.

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.
- Combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting.
- Clarification in the Technical Rationale regarding the use of VPN tunnels as a permanent connection between OEMS and/or continuous monitoring vendors who use an HMI to remotely connect to an entity SCADA system to remotely maintain in-scope sites in the context of compliance with Attachment 1, R3, Part 3.1.3.

CIP-003-11 Revisions

- Simplified VSL to align with CIP-003-10 (2016-02)
- Attachment 1, Section 3
  - Clarifying changes made to the end of Section 3.1
  - Adjustment to 3.1.3 language
  - Conforming change to 3.1.4 language in accordance with 3.1.3
  - Minor change to 3.2
- Attachment 2, Section 3
  - Conforming changes in accordance with Attachment 1, Section 3
  - Additional examples of evidence included for 3.1.2

Attachment 1, Section 3 Flow

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

3.1 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, where electronic access is:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive communications of Protection Systems;

the Responsible Entity shall implement one or more controls, **where Section 3.1. Parts (i), (ii), and (iii) are met**, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate **each user prior to** permitting access to a network(s) containing low impact BES Cyber Systems, **through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted**;

3.1.4 Protect user authentication information for user-initiated electronic access **applicable to Section 3.1.3** while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

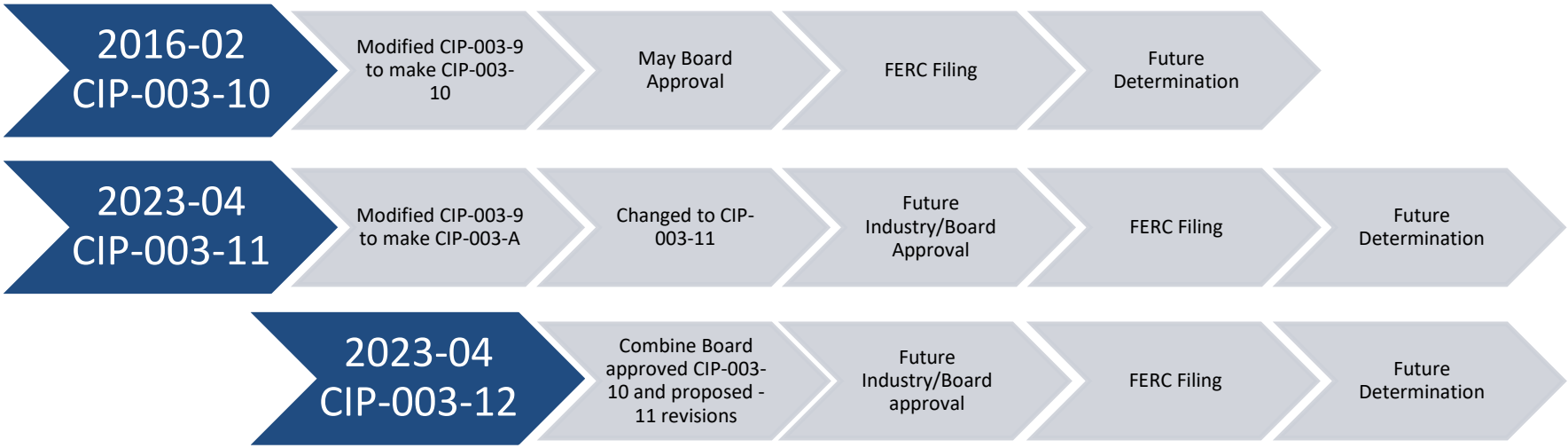
3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement **one or more control(s)** that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

CIP-003-12

- Two Drafting Teams modifying CIP-003-9 during previous ballots
  - Project 2016-02 (Virtualization) posting CIP-003-10
  - Project 2023-04 (LICRT) posting CIP-003-A
- 2016-02 changes were Board approved in May 2024
  - Project 2023-04 went from version –A to -11
- CIP-003-11 is ONLY Project 2023-04 changes (Att. 1, Section 3)
  - Still based on -9
- CIP-003-12 is an overlay of 2023-04 changes on top of the now approved -10 version *with no other changes*.
  - BOTH versions (-11 and -12) are presenting the same 2023-04 changes for ballot.

CIP-003 Version Flows



CIP-003-12 Key

CIP-003-12 - Cyber Security — Security Management Controls

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

CIP-003-12 is the combination of Project 2023-04's changes in on top of Project 2016-02's changes for virtualization. The following key describes the origin of changes in CIP-003-12:

Redline Text	Project 2023-04 original changes
Text	Project 2016-02 changes
Text	Project 2023-04 conforming changes to align with 2016-02 changes

CIP-003-12 Example

Section 3. Electronic Access Controls: ~~For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the~~Each Responsible Entity shall ~~implement~~ control electronic access ~~controls to~~as outlined below.~~:~~

3.1 ~~Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are~~For each asset containing low impact BCS identified pursuant to CIP-002 or SCI that supports a low impact BCS, where electronic access is:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

Summary of Changes

Draft

Draft 3

CIP-003-11

Clean | Redline to Last Posted | Redline to CIP-003-9 (Last Approved)

Implementation Plan

CIP-003-12

Redline to CIP-003-9

Implementation Plan

Supporting Materials

Technical Rationale

Unofficial Comment Form

VRF/VSL Justifications

Summary of Changes

Implementation Plan

- CIP-003-11 Implementation Plan
  - No changes since last posting
  - Three (3) years from regulatory approval to be compliant with 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 and procurement of new technology(s).
    - The effective date of CIP-003-9 is April 1, 2026. CIP-003-11 builds upon the implementation of CIP-003-9 for vendor remote access.

Implementation Plan

- CIP-003-12 Implementation Plan
  - General consideration – overlapping implementation timelines for CIP-003-10 and CIP-003-11
  - Effective date to be the later of:
    - 36-months after CIP-003-11 approvals; or
    - 24-months after CIP-003-12 approvals
  - Early adoption provisions from CIP-003-10 are included by reference
    - Early adoption provisions will not apply to revised language for CIP-003-11

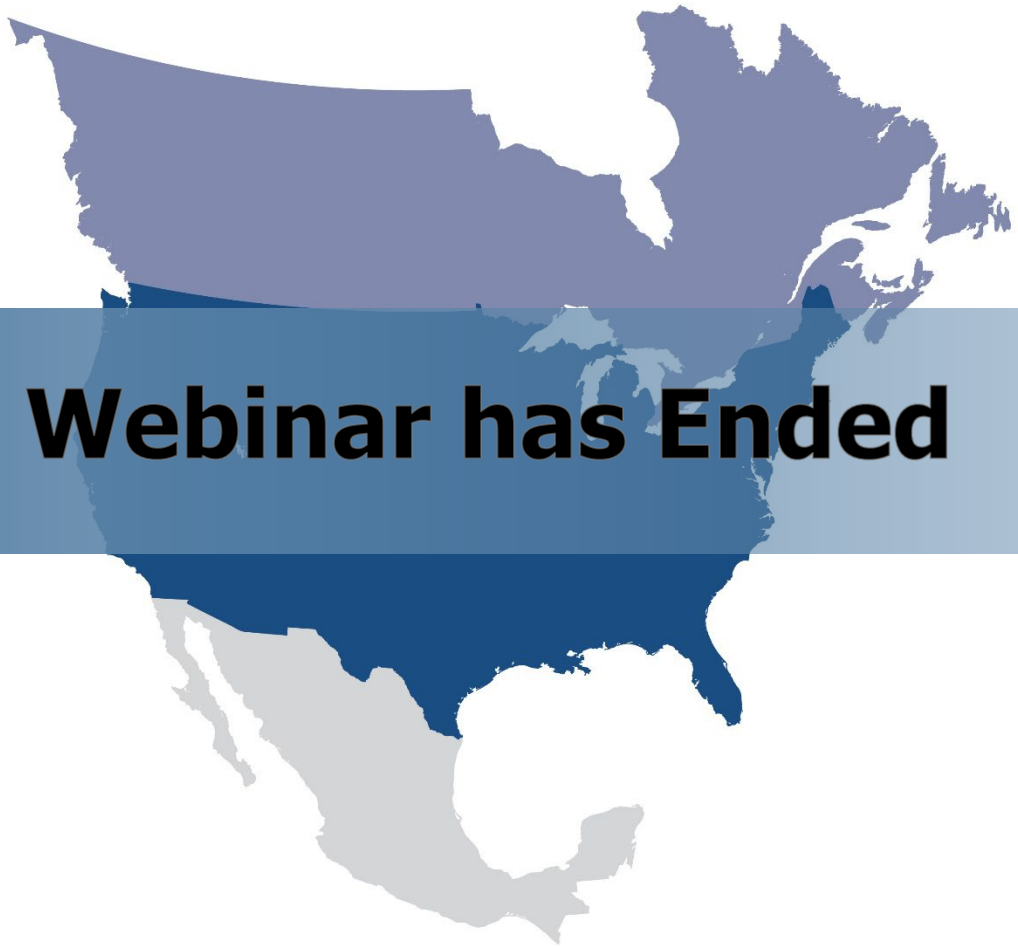
Next steps

- CIP-003-11 Posting
  - Ballot open July 2 – 11, 2024
  - Voting on CIP-003-11 and CIP-003-12 in same ballot
- Respond to Comments
  - Team Meetings in July 2024
  - Target Final Ballot at end of July 2024
  - Present to NERC Board in August 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