NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-11

Applicable Standard(s)

- CIP-003-11 – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-10 – Cyber Security – Security Management Controls[1]

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- Cyber System
- Shared Cyber Infrastructure
- Virtual Cyber Asset

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

[1] If CIP-003-10 is not currently in effect, then the currently effective version of Reliability Standard CIP-003 shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.

Background

Project 2023-04 addresses modifications to CIP-003-10 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The NERC Board of Trustees accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March 22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of CIP-003, Attachments 1 and 2 to consolidate all electronic access requirements. These revisions are captured in Reliability Standard CIP-003-11.

This implementation plan provides additional time for entities to come into compliance with Requirement R2 for the expanded scope of communications that must be monitored to detect known or suspicious malicious communications, from vendor electric remote access in CIP-003-9, to all inbound and outbound electronic access in CIP-003-11 (Attachment 1 Section 3.1.2). In determining additional time was appropriate, the Project 2023-04 drafting team considered that CIP-003-9 will become effective April 1, 2026, and two versions of the CIP-003 standard will be pending regulatory approval (CIP-003-10, CIP-003-11). The drafting team also considered that entities may have already invested significant resources to implement system architecture to monitor vendor remote access in compliance with Reliability Standard CIP-003-9, and that implementing further changes across a large fleet of low impact BES Cyber Systems may require significant additional time and investments. This implementation plan ensures that entities will have at least three years from the effective date of Reliability Standard CIP-003-9 to implement the additional controls contemplated by CIP-003-11, regardless of the date proposed Reliability Standard CIP-003-11 is approved.

The CIP-003-11 changes were made to the NERC Board of Trustees approved version of CIP-003, CIP-003-10 (Virtualization Revisions), which has been filed with the applicable governmental authorities. The use of certain defined terms within CIP-003-11 requires that the definitions for Cyber Systems, Shared Cyber Infrastructure, and Virtual Cyber Asset be approved either concurrently with or before CIP-003-11.

General Considerations

This implementation plan applies only to the CIP-003-11 revisions to the Reliability Standard that have been made by the Project 2023-04 drafting team. The implementation plan does not modify the implementation plan(s) for any other version of CIP-003.

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard CIP-003-11. This implementation plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1:

- Revise cyber security policy, plan, 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.

Effective Date

Reliability Standard CIP-003-11

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-11 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-11. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-11 within the periodic timeframes of their last performance under the version of the CIP-003 Reliability Standard then in effect.

Compliance Date for Requirement R2, Attachment 1 Section 3.1.2

Entities shall not be required to comply with Requirement R2 as it relates to the implementation of documented cyber security plan(s) addressing Attachment 1 Section 3.1.2[2] until the later of: (1) April 1, 2029; or (2) the effective date of Reliability Standard CIP-003-11.

[2] Attachment 1 Section 3.1.2: "Detect known or suspected malicious communications for both inbound and outbound electronic access."

Retirement Date

Reliability Standard CIP-003

Reliability Standard CIP-003-10, or the version of Reliability Standard CIP-003 then in effect, shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.