NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

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

Applicable Standard(s)

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

Requested Retirement(s)

- CIP-003-9 – Cyber Security – Security Management Controls

Prerequisite Standard(s)

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

- None

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

Background

Project 2023-04 addresses modifications to CIP-003-9 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 Board 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 Attachment 1 to consolidate all electronic access, with sub-sections providing additional requirements based on the type of access (Vendor, dial-up, local, etc.).

General Considerations

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard. 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 and procurement of new technology(s).
- Install new technology(s) at all assets containing low impact BES Cyber Systems.
- The effective date of CIP-003-9 is April 1, 2026. The cyber security controls implemented with CIP-003-A do not conflict and build upon the implementation of CIP-003-9 for vendor electronic remote access.

Effective Date

Reliability Standard CIP-003-A

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-A as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-A. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-A within the periodic timeframes of their last performance under CIP-003-9.

Retirement Date

Reliability Standard CIP-003-9

Reliability Standard CIP-003-9 shall be retired immediately prior to the effective date of CIP-003-A in the particular jurisdiction in which the revised standard is becoming effective.