NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Reliability Coordinator
- Transmission Operator
- Transmission Owner
- Facilities[2]

Background

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the

[1] See subject standards for additional information on Distribution Providers subject to the standards.
[2] See subject standards for additional information on Facilities subject to the standards.

proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

General Considerations

This standard will become effective 18 months following regulatory approval. The 18-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Address the increased scope of the CIP-011 "Applicability" column now present in the updated Requirement R1 and new Requirement R2, which is focused on protection of BCSI. ;
- Implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services;
- Develop a risk management method(s) to evaluate vendors' environments for data governance and rights management; identity and access management; security management (physical and cyber); and application, infrastructure, and network security; and
- Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011.

The 18-month implementation period will allow budgetary cycles for Responsible Entities to allocate the proper amount of resources to support implementation of the updated CIP-004 and CIP-011. In addition, the implementation period will provide ERO and Responsible Entities flexibility in case of unforeseen circumstances or events and afford the opportunity for feedback to be provided to the ERO and Responsible Entities through various communication vehicles within industry (e.g., NERC Reliability Standards Technical Committee, North American Transmission Form), which will encourage more ownership and commitment by Responsible Entities to adhere to the updated CIP-004 and CIP-011.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-3 – Cyber Security - Information Protection

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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

CIP-004-6 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-2 – Cyber Security - Information Protection

Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.