NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2021-03 CIP-002 | Reliability Standard CIP-002-Y

Applicable Standard(s)

- Reliability Standard CIP-002-Y – Cyber Security -Bulk Electric System (BES) Cyber System Categorization

Requested Retirement(s)

- Reliability Standard CIP-002-5.1a – Cyber Security - BES Cyber System Categorization

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

Modified Terms in the NERC Glossary of Terms

This section includes all newly defined, revised, or retired terms used or eliminated in the NERC Reliability Standard. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Proposed Modified Definition(s):

Control Center – One or more rooms where a responsible entity hosts operating personnel to monitor and control the BES in real-time, as described below, including any spaces that house the Cyber Assets used by operating personnel to monitor and control the BES in real-time. Cyber Assets used by operating personnel to monitor and control the BES in real-time are generally housed in a centralized location and exclude field assets such as remote terminal units.

(1) Operating personnel who perform the Real-time reliability-related tasks of a Reliability Coordinator;

(2) Operating personnel who perform the Real-time reliability-related tasks of a Balancing Authority;

(3) Operating personnel who perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations;

(4) Operating personnel of a Transmission Owner who have the capability to electronically control Transmission Facilities at two or more locations in real-time; or

(5) Operating personnel of a Generator Operator who have the capability to electronically control generation Facilities at two or more locations in real-time.

Background

Project 2021-03 addresses modifications to Reliability Standard CIP-002-5.1a to clarify the characterization of BES Cyber Systems associated with Control Centers used to perform the functional obligations of the Transmission Operator. Specifically, Project 2021-03 includes revisions to CIP-002 Criterion 2.12 in Attachment 1 and the Control Center definition. The proposed revisions to Attachment 1 address the categorization of Transmission Owner Control Centers performing the functional obligations of a Transmission Operator. These modifications resulted from recommendations from the CIP-002 Transmission Owner Control Center Field Test Report.[1]

General Considerations

This Implementation Plan includes phased-in implementation dates for Criterion 2.12 of CIP-002-Y, Attachment 1. The phased-in implementation dates allow Responsible Entities[2] a longer implementation period if the revisions to the criterion would result in a higher impact level categorization of a BES Cyber System.

Effective Date and Phased-In Compliance Dates

The effective date for proposed Reliability Standard CIP-002-Y and the modified definition is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion of it), the additional time for compliance with that section is specified below. The phased-in implementation date for those particular sections is the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

[1] The final field test report is available at https://www.nerc.com/pa/Stand/Project202103_CIP002_Transmission_Owner_Control_Ce/2021-03_CIP-002_TOCC_Field_Test_Final_Report_01262023.pdf.

[2] As used in the CIP Reliability Standards, a Responsible Entity refers to a registered entity responsible for the implementation of and compliance with a particular requirement.

Reliability Standard CIP-002-Y – Cyber Security – BES Cyber System Categorization

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 three (3) 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 three (3) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Dates for CIP-002-Y

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in CIP-002-Y, Requirement R2 within 15 calendar months of their last performance of Requirement R2 under CIP-002-5.1a.

Phased-in Implementation Date for CIP-002-Y, Requirement R1, Attachment 1 Criterion 2.12

If the revisions to Criterion 2.12 of Attachment 1 to CIP-002-Y result in a higher impact level categorization of a BES Cyber System, the Responsible Entity shall not be required to identify that BES Cyber System as that higher categorization nor apply the requirements throughout the CIP standards applicable to that higher categorization until 24 months after the effective date of CIP-002-Y. Until that time, the Responsible Entity shall continue to identify that BES Cyber System consistent with its existing categorization under CIP-002-5.1a, Requirement R1, Part 1.3.

Planned or Unplanned Changes

The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5.1a shall apply to CIP-002-Y. The Implementation Plan associated with CIP-002-5.1a[3] provided as follows with respect to planned and unplanned changes (with conforming changes to the version numbers of the standard):

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-Y, Requirement R2. For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-Y, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and

[3] The Implementation Plan associated with CIP-002-5.1a is available at https://www.nerc.com/pa/Stand/Project%20200806%20Cyber%20Security%20Order%20706%20DL/Implementation_Plan_clean_4_(2012-1024-1352).pdf.

categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-5.1a Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-Y, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-Y, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-Y, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-5.1a Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes)	24 months

Control Center Definition

Where approval by an applicable governmental authority is required, the definition shall become effective on the first day of the first calendar quarter that is three (3) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-002-Y, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definition shall become effective on the first day of the first calendar quarter that is three (3) months after the date that Reliability Standard CIP-002-Y is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

Reliability Standard CIP-002-5.1a

Reliability Standard CIP-002-5.1a shall be retired immediately prior to the effective date of Reliability Standard CIP-002-Y in the particular jurisdiction in which the revised standard is becoming effective.