NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2021-03 CIP-002 | Reliability Standard CIP-002-8

Applicable Standard(s)

- Reliability Standard CIP-002-8 – Cyber Security - BES Cyber System Categorization

Requested Retirement(s)

- Reliability Standard CIP-002-7 – Cyber Security - BES Cyber System Categorization

Prerequisite Definition

This definition must be approved before the Applicable Standard becomes effective:

- Cyber System[1]

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

Control Center - One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator

[1] The new term Cyber System was developed as part of Project 2016-02 – Modifications to CIP Standards.

for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

OR

One or more facilities of a Transmission Owner that have the capability to control transmission Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated data centers, and excluding field Cyber Assets used for telemetry.

Background

Project 2021-03 includes revisions to the Control Center definition and CIP-002 Attachment 1. The proposed revisions to the Control Center definition are intended to ensure Transmission Owners correctly identify their Control Centers. The proposed revisions to Attachment 1 address the categorization of Transmission Owner Control Centers that have the capability to control transmission Facilities at two or more locations in real-time using SCADA. These modifications resulted from recommendations from the CIP-002 Transmission Owner Control Center Field Test Report.[2]

General Considerations

This Implementation Plan includes phased-in implementation dates for CIP-002-8, Attachment 1. The phased-in implementation dates allow Responsible Entities[3] 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-002-8 and the modified definition is provided below. Where the drafting team identified the need for a longer implementation period for compliance with a particular section of the 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.

Reliability Standard CIP-002-8 and Control Center Definition

Where approval by an applicable governmental authority is required, the standard and Control Center definition shall become effective on the later of 1) the effective date of CIP-002-7; or 2) 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 CIP-002-8, or as otherwise provided for by the applicable governmental authority.

[2] 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

[3] 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.

Where approval by an applicable governmental authority is not required, the standard and Control Center definition shall become effective on the later of 1) the effective date of CIP-002-7; or 2) the first day of the first calendar quarter that is three (3) months after the date CIP-002-8 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Dates for CIP-002-8

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in CIP-002-8, Requirement R2 within 15 calendar months of their last performance of Requirement R2 under the version of CIP-002 immediately effective prior to CIP-002-8.

Phased-in Implementation Date for CIP-002-8, Requirement R1, Attachment 1 Criterion 2.12

If the revisions to Criteria 2.12 of Attachment 1 to CIP-002-8 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- 002-8. This would be considered a planned change, such that the Responsible Entity is expected to comply with the higher categorization 24 months after the effective date of CIP-002-8 as opposed to further extensions that would be allowable for an unplanned change. Until that time, the Responsible Entity shall continue to identify that BES Cyber System consistent with its existing categorization under CIP-002-5.1a or CIP-002-7, Requirement R1, Part 1.3, whichever version of CIP-002 is enforceable immediately prior to the effective date of CIP-002-8.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or a BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-8, 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-002-8, 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 categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control or Monitoring Systems and Protected Cyber Assets, etc. For periodic requirements in Reliability Standards CIP-004 through CIP-011, the period within which Responsible Entities must initially comply begins on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control or Monitoring Systems and Protected Cyber Assets.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or a BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-8, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-8, Attachment 1, then 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-002-8, 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 or Monitoring Systems and Protected Cyber Assets, etc. For periodic requirements in Reliability Standards CIP-004 through CIP-011, the period within which Responsible Entities must initially comply begins at the end of the timelines listed below.

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

Retirement Date

Reliability Standard CIP-002-7

Reliability Standard CIP-002-7 shall be retired immediately prior to the effective date of Reliability Standard CIP-002-8 in the particular jurisdiction in which the revised standard is becoming effective.