NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-002-6

Applicable Standard(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization

Requested Retirement(s)

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

Prerequisite Standard(s) or Definitions

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

General Considerations

This Implementation Plan includes a phased-in implementation dates for Criterion 2.12 of CIP-002-6, Attachment 1. The phased-in implementation dates allow Responsible Entities[1] 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 Implementation Dates

The effective date for proposed Reliability Standard CIP-002-6 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),

[1] 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.

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-002-6 – 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 immediately 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 immediately 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
Responsible Entities shall initially comply with the periodic requirements in CIP-002-6, Requirement R2 within 15 calendar months of their last performance of Requirement R2 under CIP-002-5.1a.

Phased-in Implementation Date for CIP-002-6, Requirement R1, Attachment 1 Criterion 2.12
If the revisions to Criterion 2.12 of Attachment 1 to CIP-002-6 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-002-6. 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 shall apply to CIP-002-6. The Implementation Plan associated with CIP-002-5 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-002-6, 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-002-6, 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 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* above.

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-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, 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-002-6, 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* above.

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	24 months

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	

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-002-6 in the particular jurisdiction in which the revised standard is becoming effective.