NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

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

Applicable Standard

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

Requested Retirements

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

Prerequisite Standard

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

Effective Date

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

Where approval by an applicable governmental authority is required, Reliability Standard CIP-002-6 shall become effective on 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, Reliability Standard CIP-002-6 shall become effective sixty (60) days following the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned and Unplanned Changes

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the assessment under CIP-002-6, Requirement R2, which were planned and implemented by the responsible entity.

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 applicable CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the assessment under CIP-002-6, Requirement R2, which were not planned by the responsible entity. 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 *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the applicable 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. Initial performance of periodic requirements shall occur by the end of the specified period following the update of the identification and categorization of the affected BES Cyber System. For example, initial performance shall be within 15 months following the update of the identification and categorization of the affected BES Cyber System for requirements that must be performed at least once every 15 calendar months.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the applicable 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. Initial performance of periodic requirements shall occur by the end of the specified period following the update of the identification and categorization of the affected BES Cyber System.

Scenario of Unplanned Changes	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 from low impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high 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-002-6 identification and categorization processes)	24 months

For the purposes of transitioning from CIP-002-5.1a to CIP-002-6, increases in BES Cyber System categorization (i.e., from low to medium/high or from medium to high) from the application of CIP-002-6 Attachment 1 criteria are provided 24 months for implementation of applicable CIP Cyber-Security Standards.

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.