NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

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 that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 12 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 12 months after the date the Reliability 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 Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

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 Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.