NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard

Applicable Standard(s)

CIP-005-6 — Cyber Security — Electronic Security Perimeters

CIP-010-3 — Configuration Change Management and Vulnerability Assessments

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

CIP-005-5 — Cyber Security — Electronic Security Perimeters

CIP-010-2 — Configuration Change Management and Vulnerability Assessments

Prerequisite Standard(s)

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

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 apply only to BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations. Order No. 829 (at P 2) states:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

FERC directed NERC to submit the new or modified Reliability Standard(s) within one year of the effective date of Order No. 829, i.e., by September 27, 2017.

General Considerations

Consistent with the directive to develop a forward-looking Reliability Standard, the implementation of Reliability Standards in Project 2016-03 do not require the abrogation or re-negotiation of contracts (including amendments to master agreements and purchase orders) with vendors, suppliers or other entities executed as of the effective date of the proposed Reliability Standards (See FERC Order No. 829, P. 36).

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-1.

Effective Date

For all Reliability Standards in Project 2016-03 — CIP-005-6, CIP-010-3, and CIP-013-1

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 18 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 18 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

CIP-013-1 Requirement R3
The initial review and approval of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement R3 must be completed on or before the effective date of CIP-013-1.

Planned or Unplanned Changes Resulting in a Higher Categorizaton

Compliance timelines with CIP-005-6, CIP-010-3, and CIP-013-1 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards.

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5 (or any subsequent version of that Reliability Standard) 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-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, 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-002-5, 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-002-5, Attachment 1, criteria.

For planned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 on the update of the identification and categorization of the affected BES Cyber System.

For unplanned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 according to the following timelines, following the identification and categorization of the affected BES Cyber System.

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 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-002-5 identification and categorization processes)	24 Months

Retirement Date

Standards listed in the **Requested Retirement(s)** section shall be retired immediately prior to the effective date in the particular jurisdiction in which the revised standards are becoming effective.