Implementation Plan
Project 2016-03 Cyber Security Supply Chain Risk Management
Reliability Standard CIP-013-1

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 AssessmentsNone

Prerequisite Standard(s)
None

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

- 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

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 the Reliability Standards in Project 2016-03 CIP-013-1 does not require the abrogation or renegotiation 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 CIP-013-1 (See FERC Order No. 829, P. 36).

Contracts entering the Responsible Entity’s procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

Effective Date

CIP-013-1 — Cyber Security — Supply Chain Risk Management
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 standards Standards shall become effective on the first day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority’s order approving the
Reliability standards, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability standards shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the Reliability standards 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 R2R3
The initial review and approval and update, as necessary, of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement R2-R3 must be completed on or before within fifteen (15) calendar months of the effective date of CIP-013-1.

Definition
None

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. None