

# Implementation Plan

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

### Applicable Standard(s)

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

### Requested Retirement(s)

None

### 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 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 CIP-013-1 does not require the abrogation or re-negotiation of contracts with vendors, suppliers or other entities executed as of the effective date of CIP-013-1 (See FERC Order No. 829, P. 36).

## Effective Date

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

Where approval by an applicable governmental authority is required, the standard 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 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 that is twelve (12) months 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

### Requirement R2

The initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 must be completed within fifteen (15) calendar months of the effective date of CIP-013-1.

**Definition**

None

**Retirement Date**

None