Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of the proposed standard

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 18, 2016

Anticipated Actions	Date
45-day formal comment period with ballot	January 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

When this standard receives Board adoption, the rationale boxes will be moved to the Supplemental Material Section of the standard.

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate risks of cyber security incidents affecting the reliable operation of the Bulk Electric System (BES) by implementing security controls in the supply chain for BES Cyber Assets and computing and networking services that impact BES operations.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. 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.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. 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.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Date: See Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cybersecurity risk management plan(s) that set forth the controls used to collectively address the following supply chain cybersecurity objectives for BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Software integrity and authenticity controls that address risks from compromised software and firmware. The controls shall provide for verification of the following prior to installation:

1.1.1. The identity of the publisher for software and firmware, and any upgrades and patches to software and firmware;

1.1.2. The integrity of software and firmware upgrades and patches.

1.2. Remote access controls to address risks from compromised third-party access credentials and risks of a compromise at a vendor or service provider from traversing over an unmonitored remote access connection. The controls shall provide for:

1.2.1. Controlling third-party initiated remote access, including machine-to-machine remote access;

1.2.2. Monitoring third-party remote access, including machine-to-machine remote access; and

1.2.3. Detecting and responding to unauthorized third-party remote access activity.

1.3. Information system planning controls to address the consideration of cyber security supply chain risks in information system development. The controls shall:

1.3.1. Assess risks that may be introduced by a third-party; and

1.3.2. Evaluate methods to address identified third-party risk.

1.3.3. [*Should the standard address implementation here? Or should implementation be covered in Requirement R2?*]

1.4. Procurement controls to identify and verify security controls used by vendors or service providers in delivering products or services. These procurement controls should address the following security controls used by the vendor or service provider:

1.4.1. Notification of security events that may impact the Responsible Entity;

1.4.2. Notification when employees should no longer be granted remote or onsite access due to employment termination, reassignment, or transfer;

1.4.3. Disclosure of known vulnerabilities that may impact the Responsible Entity; and

1.4.4. Coordination of response to vendor-related cyber security incidents affecting the Responsible Entity .

M1. Evidence shall include one or more documented supply chain cybersecurity risk management plan(s) that collectively include the controls used to address the security objectives identified in Requirement R1.

R2. Each Responsible Entity shall implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts. *[Violation Risk Factor:] [Time Horizon: Operations Planning]*

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cybersecurity risk management plan(s) as specified in the Requirement. This evidence could include, but is not limited to, dated contracts or written agreements in electronic or hard copy format.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate(s) approval at least once every 15 calendar months of the security controls set forth in the supply chain cybersecurity risk management plan(s) used to address the security objectives identified in Requirement R1. The review of the security controls shall include the consideration of new risks and mitigation measures and the identification of related changes, if any, made to the controls. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the security controls approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the security controls by the CIP Senior Manager or delegate(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The [applicable entity(ies)] shall keep data or evidence of Requirement X for X calendar days/months/years.

1.3. Compliance Monitoring and Enforcement Program
As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.				
R2.				
R3.				

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 829	NA

Standard Attachments

None

Guidelines and Technical Basis

See Technical Reference Document

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT adoption, the text from the rationale text boxes was moved to this section.