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 21, 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

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

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

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

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

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

4.2.2.1. 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

Rationale for Requirement R1:
The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes controls for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to BES Cyber Systems and, to the extent applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan.

Requirement R1 Part 1.1 addresses Order No. 829 directives for identification and documentation of risks in the planning and development processes related to proposed BES Cyber Systems (P. 56). The objective is to ensure entities consider risks and options for mitigating these risks when planning, acquiring, and deploying BES Cyber Systems.

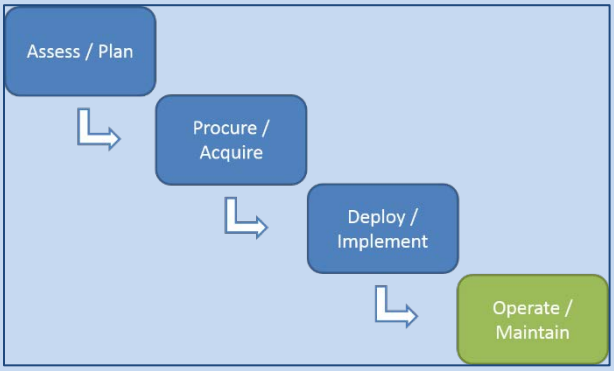
Requirement R1 Part 1.2 addresses Order No. 829 directives for procurement controls to address vendor-related security concepts in future contracts for BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 is accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to ensure that the software being installed in the applicable cyber system was not modified without the awareness of the software supplier and is not counterfeit.

The term *vendors* as used in the standard includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of Requirement R1 and R2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle.

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. The use of controls in BES Cyber System planning and development to:

1.1.1. Identify and assess risk(s) during the procurement and deployment of vendor products and services; and

1.1.2. Evaluate methods to address identified risk(s).

1.2. The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:

1.2.1. Process(es) for notification of vendor security events;

1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3. Process(es) for disclosure of known vulnerabilities;

1.2.4. Coordination of response to vendor-related cyber security incidents;

1.2.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

1.2.6. Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

1.2.7. Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

M1. Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for mitigating cyber security risks as specified in the Requirement; and (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk management plan(s).

Rationale for Requirement R2:
The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Order No. 829 also directs that the periodic assessment "ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities" (P. 47). Examples of sources of information that the entity considers include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

R2. Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

2.1. Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and

2.2. Obtaining CIP Senior Manager or delegate approval.

M2. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s) and evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures as specified in the Requirement. 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 supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

Rationale for Requirement R3:
The proposed requirement addresses Order No. 829 directives for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

3.1. Operating System(s);

3.2. Firmware;

3.3. Commercially available or open-source application software; and

3.4. Patches, updates, and upgrades to 3.1 through 3.3.

M3. Evidence shall include (i) a documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation that the entity performed the actions contained in the process to verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to installation on high and medium impact BES Cyber Systems.

Rationale for Requirement R4:
The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective of the Requirement is to mitigate potential risks of a compromise at a vendor from traversing over an unmonitored remote access connection.

The objective of Requirement R4 Part 4.3 is for entities to have the ability to rapidly disable remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **4.1.** Authorization of remote access by the Responsible Entity;
- **4.2.** Logging and monitoring of remote access sessions to detect unauthorized activity; and
- **4.3.** Disabling or otherwise responding to unauthorized activity during remote access sessions.

M4. Evidence shall include (i) a documented process(es) for controlling vendor remote access as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation of authorization of vendor remote access; hard copy or electronic logs of vendor-initiated Interactive Remote Access and system-to-system remote access sessions; hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.

Rationale for Requirement R5:
The proposed requirement addresses Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems. (P. 48 and P. 51).

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

An entity could apply process(es) used for Requirements R3 and R4 to satisfy its obligations in Requirement R5 or could develop a separate policy or process(es) to address low impact BES Cyber Systems.

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

5.1. Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and

5.2. Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).

M5. 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 or delegate for each cyber security policy.

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 Responsible 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.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

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.	N/A	N/A	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include one of the elements specified in Parts 1.1 or 1.2.	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include either of the elements specified in Parts 1.1 or 1.2.; OR The Responsible Entity did not implement one or more documented supply chain risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 17 calendar months but less than or equal to 18	The Responsible Entity did not review and update, as necessary, its supply chain cyber security risk management plan(s) and obtain CIP Senior Manager or delegate approval within 18 calendar months of the previous review as specified in the Requirement.

	since the previous review as specified in the Requirement.	since the previous review as specified in the Requirement.	calendar months since the previous review as specified in the Requirement.	
R3.	N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.
R4.	N/A	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include one of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include two of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include any of the elements specified in Part 4.1 through Part 4.3; OR, The Responsible Entity did not implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems as

				specified in the Requirement.
R5.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 16 calendar months but less than or equal to 17 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include one of the elements in Parts 5.1 or 5.2; OR The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 17 calendar months but less than or equal to 18 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include either of the elements in Parts 5.1 or 5.2; OR The Responsible Entity did not have cyber security policies that were reviewed and approved by the CIP Senior Manager or delegate as specified in the requirement.

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

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.