A. Introduction

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

2. **Number:** **CIP-013-3**

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 (BCS).

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-013-3:

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

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

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. 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.

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

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. 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). 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.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) 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 CEA 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 CEA 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.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.
R2.	The Responsible Entity did not implement one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity did not implement the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				procuring applicable systems as specified in Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 16th calendar month since the previous review.	The Responsible Entity exceeded the 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 17th calendar month since the previous review.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 18th calendar month since the previous review.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17		Respond to FERC Order No. 829.
1	08/10/17	Adopted by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	11/05/2020	Adopted by the NERC Board of Trustees.	Modified to address directive in FERC Order No. 850.
2	3/18/2021	FERC Order approving CIP-013-2. Docket No. RD21-2-000.	
3	5/9/2024	Adopted by the NERC Board of Trustees	Virtualization Modifications