

Alberta Reliability Standard

Cyber Security – Supply Chain Risk Management

CIP-013-AB-2



A. Introduction

1. Title: Cyber Security - Supply Chain Risk Management

2. Number: CIP-013-AB-2

3. Purpose: To mitigate cyber security risks to the reliable operation of the **bulk electric system** 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. [Intentionally left blank.]

4.1.2. a **legal owner** of an **electric distribution system** that owns one or more of the following facilities, systems, and equipment for the protection or restoration of the **bulk electric system**:

4.1.2.1. Each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. Is part of a load shedding program that is subject to one or more requirements in a **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** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**; and

4.1.2.3. Each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to an **electric distribution system** where the **protection system** is subject to one or more requirements in a **reliability standard**.

4.1.3. the **operator** of a **generating unit** that is part of the **bulk electric system** and the **operator** of an **aggregated generating facility** that is part of the **bulk electric system**;
4.1.4. the **legal owner** of a **generating unit** that is part of the **bulk electric system** and the **legal owner** of an **aggregated generating facility** that is part of the **bulk electric system**;

4.1.5. [Intentionally left blank.]

4.1.6. the **operator** of a **transmission facility**;

4.1.7. the **legal owner** of a **transmission facility**; and

4.1.8. the **ISO**.

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. Legal owner of an electric distribution system and legal owner of a transmission facility: One or more of the following facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner of an electric distribution system** or a **legal owner of a transmission facility** for the protection or restoration of the **bulk electric system** :

4.2.1.1. Each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. Is part of a load shedding program that is subject to one or more requirements in a **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 **remedial action scheme** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**.

4.2.1.3. Each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to any **transmission facility** or **electric distribution system** where the **protection system** is subject to one or more requirements in a **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 **point of connection** of the starting station service of the next **generating unit(s)** or **aggregated generating facility(ies)** to be started.

4.2.2. Responsible Entities listed in 4.1 other than a **legal owner of an electric distribution system**: all **bulk electric system** facilities

4.2.3. Exemptions: The following are exempt from CIP-013-AB-2:

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**.

4.2.3.3. [Intentionally left blank.]

4.2.3.4. For the **legal owner of an electric distribution system**, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. 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-AB-5.1 or any subsequent version of that **reliability standard**.

5. Effective Date: . *To be determined in consultation with stakeholders.*

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 **BES cyber systems** and their associated **electronic access control or monitoring systems** and **physical access control systems**. 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 **BES cyber systems** and their associated **electronic access control or monitoring systems** and **physical access control systems** to identify and assess cyber security risk(s) to the **bulk electric system** 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 **BES cyber systems**, and their associated **electronic access control or monitoring systems** and **physical access control systems**, 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 for use in the **BES cyber system** and their associated **electronic access control or monitoring systems** and **physical access control systems**; 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.

Alberta Reliability Standard

Cyber Security – Supply Chain Risk Management

CIP-013-AB-2



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 **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 **months**; and documented approval by the **CIP senior manager** or delegate.

C. Compliance

[Intentionally left blank.]

D. Regional Variances

None.

E. Associated Documents

- CIP-013-2 Technical Rationale

Version History

Version	Effective Date	Description of Change
2	TBD	Initial Version