Alberta Reliability Standard
Cyber Security – Information Protection
CIP-011-AB-3

A. Introduction

1. Title: Cyber Security – Information Protection

2. Number: CIP-011-AB-3

3. Purpose: To prevent unauthorized access to **BES cyber system information** by specifying information protection requirements in support of protecting **BES cyber systems** against compromise that could lead to misoperation or instability in the **bulk electric system**.

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 **reliability 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**;

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**; and

4.1.2.4. 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.

4.1.3. 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 **reliability standard** where a specific type of facilities, systems, 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 **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 **reliability standard** CIP-011-AB-3

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 CIP-002 identification and categorization processes.

5. Effective Dates**:** See CIP-PLAN-AB-3, *Cyber Security Implementation Plan for CIP Cyber Security Reliability Standards*.

6. Background**: Reliability standard** CIP-011 exists as part of a suite of CIP **reliability standards** related to cyber security, which require the initial identification and categorization of **BES cyber systems** and require a minimum level of organizational, operational, and procedural controls to mitigate risk to **BES cyber systems**.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the **reliability standards** include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security **reliability standards** could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the **reliability standards**.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact **BES cyber systems**. For example, a single training program could meet the requirements for training personnel across multiple **BES cyber systems**.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the **reliability standards**, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for **underfrequency load shedding** and **under voltage load shed**. This particular threshold of 300 MW for **under voltage load shed** and **underfrequency load shedding** was provided in Version 1 of the NERC CIP Cyber Security **reliability standards**. The threshold remains at 300 MW since it is specifically addressing **under voltage load shed** and **underfrequency load shedding**, which are last ditch efforts to save the **bulk electric system**. A review of **underfrequency load shedding** tolerances defined within **reliability standards** for **underfrequency load shedding** program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable **underfrequency load shedding** operational tolerances.

"Applicable Systems" Columns in Tables**:**

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- High Impact **BES Cyber Systems** – Applies to **BES cyber systems** categorized as high impact according to the CIP-002-AB-5.1 and any amendments made thereto from time to time identification and categorization processes.

- Medium Impact **BES Cyber Systems** – Applies to **BES cyber systems** categorized as medium impact according to the CIP-002-AB-5.1 and any amendments made thereto from time to time identification and categorization processes.

- **Electronic Access Control or Monitoring Systems** – Applies to each **electronic access control or monitoring system** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems** – Applies to each **physical access control system** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**.

- **Protected Cyber Assets** – Applies to each **protected cyber asset** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system.**

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for **BES cyber system information** pertaining to "Applicable Systems" identified in *CIP-011-AB-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-AB-3 Table R1 – Information Protection Program*. *[Alberta Risk Rating: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-AB-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-AB-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	Method(s) to identify **BES cyber system information**.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify **BES cyber system information** from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify **BES cyber system information** as designated in the entity's information protection program; or

CIP-011-AB-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Training materials that provide personnel with sufficient knowledge to identify **BES cyber system information**; or • Storage locations identified for housing **BES cyber system information** in the entity's information protection program.
1.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	Method(s) to protect and securely handle **BES cyber system information** to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise **BES cyber system information** may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of **BES cyber system information**; or • Records indicating that **BES cyber system information** is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise **BES cyber system information** may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic **BES cyber system information** (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical **BES cyber system information** (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to

CIP-011-AB-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			protect **BES cyber system information** (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-AB-3 Table R2 – BES cyber asset Reuse and Disposal*. *[Alberta Risk Rating: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-AB-3 Table R2 – BES cyber asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-AB-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	Prior to the release for reuse of applicable **cyber assets** that contain **BES cyber system information** (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of **BES cyber system information** from the **cyber asset** data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of **BES cyber system information** such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the **physical security perimeter** or other methods used to prevent unauthorized retrieval of **BES cyber system information**.

CIP-011-AB-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	Prior to the disposal of applicable **cyber assets** that contain **BES cyber system information**, the Responsible Entity shall take action to prevent the unauthorized retrieval of **BES cyber system information** from the **cyber asset** or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable **cyber asset**; or • Records of actions taken to prevent unauthorized retrieval of **BES cyber system information** prior to the disposal of an applicable **cyber asset**.

C. Compliance

[Intentionally left blank.]

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

- CIP-PLAN-AB-3, *Cyber Security – Implementation Plan* for CIP Cyber Security Reliability Standards and any amendments made thereto from time to time.
- AESO Information Document, #2015-003RS*, Guidance Information for CIP Standards* and any amendments made thereto from time to time.

Version History

Version	Effective Date	Description of Changes
1	Oct 1, 2017	Initial Version
3	April 1, 2026	Addresses directives from FERC Order No. 791. Revised to enhance BES reliability for entities to manage their BES cyber system information.