Alberta Reliability Standard
Cyber Security – Security Management Controls
CIP-003-AB-5

A. Introduction

1. Title: Cyber Security – Security Management Controls

2. Number: CIP-003-AB-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect **BES cyber systems** against compromise that could lead to misoperation or instability in the **bulk electric system**.

4. Applicability:

4.1. For the purpose of the requirements contained herein, the following list of entities will be collectively referred to as "Responsible Entities". For requirements in this **reliability standard** where a specific entity or subset of entities are the applicable entity or entities, the 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 entity in subsection 4.1.2., 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 transmission 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 contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.1.3. the **operator** of a **generating unit** and the **operator** of an **aggregated generating facility**;

4.1.4. the **legal owner** of a **generating unit** and the **legal owner** of an **aggregated generating facility**;

4.1.5. [Intentionally left blank.]

4.1.6. [Intentionally left blank.]

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

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

4.1.9. the **ISO**.

4.2. For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in subsection 4.1 above are those to which these requirements are applicable. For requirements in this **reliability 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. 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 one or more of the entities in subsection 4.2.1, 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 where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.2.1.4. each **cranking path** and group of elements meeting the initial switching requirements from a contracted **blackstart resource** up to and including the first **point of supply** and/or **point of delivery** of the next **generating unit** or **aggregated generating facility** to be started;

4.2.2. Responsible Entities listed in subsection 4.1 other than a **legal owner** of an **electric distribution system** are responsible for:

4.2.2.1. each **transmission facility** that is part of the **bulk electric system** except each **transmission facility** that:

4.2.2.1.1. is a transformer with fewer than 2 windings at 100 kV or higher and does not connect a contracted **blackstart resource**;

4.2.2.1.2. radially connects only to load;

4.2.2.1.3. radially connects only to one or more **generating units** or **aggregated generating facilities** with a combined **maximum authorized real power** of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**; or

4.2.2.1.4. radially connects to load and one or more **generating units** or **aggregated generating facilities** that have a combined **maximum authorized real power**

of less than or equal to 67.5 MW and does not connect a contracted **blackstart resource**;

4.2.2.2. a **reactive power** resource that is dedicated to supplying or absorbing **reactive power** that is connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, except those **reactive power** resources operated by an end-use customer for its own use;

4.2.2.3. a **generating unit** that is:

4.2.2.3.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;

4.2.2.3.2. within a power plant which:

4.2.2.3.2.1. is not part of an **aggregated generating facility**;

4.2.2.3.2.2. is directly connected to the **bulk electric system**; and

4.2.2.3.2.3. has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;

4.2.2.3.3. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.3.4. a contracted **blackstart resource**;

4.2.2.4. an **aggregated generating facility** that is:

4.2.2.4.1. directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;

4.2.2.4.2. within an industrial complex with **supply transmission service** greater than 67.5 MW; or

4.2.2.4.3. a contracted **blackstart resource**;

and

4.2.2.5. **control centres** and backup **control centres**.

4.2.3. The following are exempt from this **reliability standard**:

4.2.3.1. [Intentionally left blank.]

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 subsection 4.2.1 above.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

B. Requirements and Measures

R1. Each Responsible Entity, for its High Impact and Medium Impact **BES cyber systems**, shall review and obtain **CIP senior manager** approval at least once every 15 **months** for one or more documented cyber security policies that collectively address the following topics:

1.1 Personnel & training (CIP-004-AB-5.1);

1.2 Electronic security perimeters (CIP-005-AB-5) including **interactive remote access**;

1.3 Physical security of **BES cyber systems** (CIP-006-AB-5);

1.4 System security management (CIP-007-AB-5);

1.5 Incident reporting and response planning (CIP-008-AB-5);

1.6 Recovery plans for **BES cyber systems** (CIP-009-AB-5);

1.7 Configuration change management and vulnerability assessments (CIP-010-AB-1);

1.8 Information protection (CIP-011-AB-1); and

1.9 Declaring and responding to **CIP exceptional circumstances**.

M1. Examples of evidence may include, but are 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 **months**; and documented approval by the **CIP senior manager** for each cyber security policy.

R2. Each Responsible Entity for its assets identified in CIP-002-AB-5.1, requirement R1, part 1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain **CIP senior manager** approval for those policies at least once every 15 **months**:

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and **dial-up connectivity**; and

2.4 Incident response to a **cyber security incident**.

An inventory, list, or discrete identification of Low Impact **BES cyber systems** or their **BES cyber assets** is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; 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 **months**; and documented approval by the **CIP senior manager** for each cyber security policy.

R3. Each Responsible Entity shall identify a **CIP senior manager** by name and document any change within 30 **days** of the change.

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the **CIP senior manager**.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP **reliability standards**, the **CIP senior manager** may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the **CIP senior manager**; and updated within 30 **days** of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

M4. An example of evidence may include, but is not limited to, a dated document, approved by the **CIP senior manager**, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Revision History

Date	Description
2017-10-01	Initial release.