# Alberta Reliability Standard
# Cyber Security – Electronic Security Perimeter(s)
# CIP-005-AB-5

## A. Introduction

1. Title: Cyber Security – Electronic Security Perimeter(s)

2. Number: CIP-005-AB-5

3. Purpose: To manage electronic access to **BES cyber systems** by specifying a controlled **electronic security perimeter** 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. 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.

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-AB-5.1 identification and

categorization processes.

5. [Intentionally left blank.]

6. [Intentionally left blank.]

## B. Requirements and Measures

**R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-AB-5 Table R1 – Electronic Security Perimeter.*

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-AB-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-005-AB-5 Table R1 – Electronic Security Perimeter | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** and their associated:<br>• **protected cyber assets** | All applicable **cyber assets** connected to a network via a routable protocol shall reside within a defined **electronic security perimeter**. | An example of evidence may include, but is not limited to, a list of all **electronic security perimeters** with all uniquely identifiable applicable **cyber assets** connected via a routable protocol within each **electronic security perimeter**. |
| 1.2 | High Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets** | All **external routable connectivity** must be through an identified **electronic access point**. | An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified **electronic access points**. |
| 1.3 | **Electronic access points** for High Impact **BES cyber systems**<br>**Electronic access points** for Medium Impact **BES cyber** | Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. | An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed |

| CIP-005-AB-5 Table R1 – Electronic Security Perimeter | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | **systems** | | and that each access rule has a documented reason. |
| 1.4 | High Impact **BES cyber systems** with **dial-up connectivity** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **dial-up connectivity** and their associated:<br>• **protected cyber assets** | Where technically feasible, perform authentication when establishing **dial-up connectivity** with applicable **cyber assets**. | An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection. |
| 1.5 | **Electronic access points** for High Impact **BES cyber systems**<br>**Electronic access points** for Medium Impact **BES cyber systems** at **control centres** | Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. | An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented. |

**R2.** Each Responsible Entity allowing Interactive Remote Access to **BES cyber systems** shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-AB -5 Table R2 – Interactive Remote Access Management.*

**M2.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-AB -5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-005-AB-5 Table R2 – Interactive Remote Access Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and | Utilize an **intermediate system** such that the **cyber asset** initiating **interactive remote access** does not directly access an applicable **cyber asset**. | Examples of evidence may include, but are not limited to, network diagrams or architecture documents. |

| CIP-005-AB-5 Table R2 – Interactive Remote Access Management | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| | their associated:<br>• **protected cyber assets** | | |
| 2.2 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets** | For all **interactive remote access** sessions, utilize encryption that terminates at an **intermediate system**. | An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates. |
| 2.3 | High Impact **BES cyber systems** and their associated:<br>• **protected cyber assets**<br>Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:<br>• **protected cyber assets** | Require multi-factor authentication for all **interactive remote access** sessions. | An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used.<br>Examples of authenticators may include, but are not limited to,<br>• something the individual knows such as passwords or PINs. This does not include User ID;<br>• something the individual has such as tokens, digital certificates, or smart cards; or<br>• something the individual is such as fingerprints, iris scans, or other biometric characteristics. |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |