

## A. Introduction

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

2. Number: CIP-005-AB-7

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. 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**;

**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 Section 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** where a specific type of

# Alberta Reliability Standard

## Cyber Security – Electronic Security

### Perimeter(s)

#### CIP-005-AB-7



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-005-AB-7:

**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:** *To be determined in consultation with stakeholders.*

**6. Background:**

**Reliability standard** CIP-005 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

# Alberta Reliability Standard

## Cyber Security – Electronic Security

### Perimeter(s)

#### CIP-005-AB-7



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 standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security 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 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 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 CIP Cyber Security 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 NERC standard drafting team 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 identification and categorization processes.

- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact **BES cyber systems** with **dial-up connectivity**.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact **BES cyber systems** with **external routable connectivity** . This also excludes **cyber assets** in the **BES cyber system** that cannot be directly accessed through **external routable connectivity** .
- **Medium Impact BES Cyber Systems** – Applies to **BES cyber systems** categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact **BES cyber systems** located at a **control centre**.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact **BES cyber systems** with **dial-up connectivity**.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact **BES cyber systems** with **external routable connectivity** . This also excludes **cyber assets** in the **BES cyber system** that cannot be directly accessed through **external routable connectivity** .
- **Protected Cyber Assets** – Applies to each **protected cyber asset** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**.
- **Electronic Access Points** – Applies at **electronic access points** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**.
- **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**.
- **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.

## 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-7 Table R1 – Electronic Security Perimeter*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-AB-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-AB-7 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact <b>BES cyber systems</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> <p>Medium Impact <b>BES cyber systems</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	<p>All applicable <b>cyber assets</b> connected to a network via a routable protocol shall reside within a defined <b>electronic security perimeter</b>.</p>	<p>An example of evidence may include, but is not limited to, a list of all <b>electronic security perimeters</b> with all uniquely identifiable applicable <b>cyber assets</b> connected via a routable protocol within each <b>electronic security perimeter</b>.</p>
1.2	<p>High Impact <b>BES cyber systems</b> with <b>external routable connectivity</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> <p>Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	<p>All <b>external routable connectivity</b> must be through an identified <b>electronic access point</b>.</p>	<p>An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified <b>electronic access points</b>.</p>
1.3	<p><b>Electronic access points</b> for High Impact <b>BES cyber systems</b></p> <p><b>Electronic access points</b> for Medium Impact <b>BES cyber systems</b></p>	<p>Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.</p>	<p>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 and that each access rule has a documented reason.</p>

CIP-005-AB-7 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact <b>BES cyber systems</b> with <b>dial-up connectivity</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> <p>Medium Impact <b>BES cyber systems</b> with <b>dial-up connectivity</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	<p>Where technically feasible, perform authentication when establishing <b>dial-up connectivity</b> with applicable <b>cyber assets</b>.</p>	<p>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.</p>
1.5	<p><b>Electronic access points</b> for High Impact <b>BES cyber systems</b></p> <p><b>Electronic access points</b> for Medium Impact <b>BES cyber systems</b> at <b>control centres</b></p>	<p>Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.</p>	<p>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.</p>

# Alberta Reliability Standard

## Cyber Security – Electronic Security Perimeter(s)

### CIP-005-AB-7



**R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-AB-7 Table R2 –Remote Access Management*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

**M2.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP- 005-AB-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-AB-7 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact <b>BES cyber systems</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> <p>Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	<p>For all <b>interactive remote access</b>, utilize an <b>intermediate system</b> such that the <b>cyber asset</b> initiating <b>interactive remote access</b> does not directly access an applicable <b>cyber asset</b>.</p>	<p>Examples of evidence may include, but are not limited to, network diagrams or architecture documents.</p>
2.2	<p>High Impact <b>BES cyber systems</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> <p>Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	<p>For all <b>interactive remote access</b> sessions, utilize encryption that terminates at an <b>intermediate system</b>.</p>	<p>An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.</p>

CIP-005-AB-7 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.3	<p>High Impact <b>BES cyber systems</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> <p>Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b> and their associated:</p> <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	<p>Require multi-factor authentication for all <b>interactive remote access</b> sessions.</p>	<p>An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used.</p> <p>Examples of authenticators may include, but are not limited to,</p> <ul style="list-style-type: none"> <li>• Something the individual knows such as passwords or PINs. This does not include User ID;</li> <li>• Something the individual has such as tokens, digital certificates, or smart cards; or</li> <li>• Something the individual is such as fingerprints, iris scans, or other biometric characteristics.</li> </ul>



CIP-005-AB-7 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.4	High Impact <b>BES cyber systems</b> and their associated: <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b> and their associated: <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	Have one or more methods for determining active vendor remote access sessions (including <b>interactive remote access</b> and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including <b>interactive remote access</b> and system-to-system remote access), such as: <ul style="list-style-type: none"> <li>• Methods for accessing logged or monitoring information to determine active vendor remote access sessions;</li> <li>• Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or</li> <li>• Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.</li> </ul>

CIP-005-AB-7 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.5	High Impact <b>BES cyber systems</b> and their associated: <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul> Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b> and their associated: <ul style="list-style-type: none"> <li>• <b>protected cyber assets</b></li> </ul>	Have one or more method(s) to disable active vendor remote access (including <b>interactive remote access</b> and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including <b>interactive remote access</b> and system-to-system remote access), such as: <ul style="list-style-type: none"> <li>• Methods to disable vendor remote access at the applicable <b>electronic access point</b> for system-to-system remote access; or</li> <li>• Methods to disable vendor <b>interactive remote access</b> at the applicable <b>intermediate system</b>.</li> </ul>

# Alberta Reliability Standard

## Cyber Security – Electronic Security Perimeter(s)

### CIP-005-AB-7



**R3.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-AB-7 Table R3 – Vendor Remote Access Management for Electronic Access Control or Monitoring Systems and Physical Access Control Systems*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

**M3.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-AB-7 Table R3 – Vendor Remote Access Management for Electronic Access Control or Monitoring Systems and Physical Access Control Systems* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-AB-7 Table R3 – Vendor Remote Access Management for Electronic Access Control or Monitoring Systems and Physical Access Control Systems			
Part	Applicable Systems	Requirements	Measures
3.1	<p><b>Electronic access control or monitoring systems and physical access control systems</b> associated with High Impact <b>BES cyber systems</b></p> <p><b>Electronic access control or monitoring systems and physical access control systems</b> associated with Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b></p>	Have one or more method(s) to determine authenticated vendor- initiated remote connections.	<p>Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as:</p> <ul style="list-style-type: none"> <li>• Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.</li> </ul>

CIP-005-AB-7 Table R3 – Vendor Remote Access Management for Electronic Access Control or Monitoring Systems and Physical Access Control Systems			
Part	Applicable Systems	Requirements	Measures
3.2	<p><b>Electronic access control or monitoring systems and physical access control systems</b> associated with High Impact <b>BES cyber systems</b></p> <p><b>Electronic access control or monitoring systems and physical access control systems</b> associated with Medium Impact <b>BES cyber systems</b> with <b>external routable connectivity</b></p>	<p>Have one or more method(s) to terminate authenticated vendor- initiated remote connections and control the ability to reconnect.</p>	<p>Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.</p>

# Alberta Reliability Standard Cyber Security – Electronic Security Perimeter(s) CIP-005-AB-7



## C. Compliance

[Intentionally left blank.]

### Regional Variances

None.

## E. Associated Documents

- CIP-005-7 Technical Rationale

### Version History

Version	Effective Date	Action	Description of Changes
5	10/1/2022		Initial Version
7	TBD		Modified to address certain directives in FERC Order No. 829 and 850.