

Alberta Reliability Standard

Cyber Security – Electronic Security

Perimeter(s)

CIP-005-AB-7



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~~BES Cyber Systems~~, by specifying a controlled electronic security perimeter~~Electronic Security Perimeter~~ in support of protecting BES cyber systems~~BES Cyber Systems~~ against compromise that could lead to misoperation or instability in the bulk electric system~~BES~~.

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.]Balancing Authority

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

4.1.2.1. Each underfrequency load shedding ~~underfrequency Load shedding (UFLS)~~ or under voltage load shed ~~undervoltage Load shedding (UVLS)~~ system that:

4.1.2.1.1. is part of a load~~Load~~ shedding program that is subject to one or more requirements in a reliability standard~~NERC or Regional Reliability Standard~~; and

4.1.2.1.2. performs automatic Load~~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 ~~Remedial Action Scheme (RAS)~~ where the remedial action scheme ~~RAS~~ is subject to one or more requirements in a reliability standard~~NERC or Regional Reliability Standard~~.

4.1.2.3. Each protection system ~~Protection System~~ (excluding underfrequency load shedding ~~UFLS~~ and under voltage load shed ~~UVLS~~) that applies to Transmission any electric distribution system where the protection system ~~Protection System~~ is subject to one or more requirements in a reliability standard~~NERC or Regional Reliability Standard~~; and

4.1.2.4. Each cranking path ~~Cranking Path~~ and group of Elements ~~elements~~ meeting the initial switching requirements from a blackstart resource ~~Blackstart Resource~~ up to and including the first point of connection ~~interconnection point~~ of the starting station service of the next generating unit(s) or aggregated generating facility(ies) ~~generation unit(s)~~ 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 ~~Generator Operator~~

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 ~~Generator Owner~~

Alberta Reliability Standard

Cyber Security – Electronic Security

Perimeter(s)

CIP-005-AB-7



- 4.1.5. ~~[Intentionally left blank.]~~**Reliability Coordinator**
- 4.1.6. ~~the operator of a transmission facility;~~**Transmission Operator**
- 4.1.7. ~~the legal owner of a transmission facility; and~~**Transmission Owner**
- 4.1.8. the ISO.**

4.2. Facilities: For the purpose of the requirements contained herein, the following ~~Facilities~~**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~~ **standard** where a specific type of ~~Facilities~~**facilities**, system, or equipment or subset of ~~Facilities~~**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: ~~Distribution Provider:~~ One or more of the following ~~Facilities~~**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~~ **the Distribution Provider** for the protection or restoration of the ~~bulk electric system~~ **BES:**

4.2.1.1. Each ~~underfrequency load shedding~~ **UFLS** or ~~under voltage load shed~~ **UVLS** ~~System- system~~ that:

4.2.1.1.1. is part of a ~~Load-load~~ shedding program that is subject to one or more requirements in a ~~reliability standard~~ **NERC or Regional Reliability Standard**; and

4.2.1.1.2. performs automatic ~~Load-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~~ **RAS** where the ~~remedial action scheme~~ **RAS** is subject to one or more requirements in a ~~reliability standard~~ **NERC or Regional Reliability Standard**.

4.2.1.3. Each ~~protection system~~ **Protection System** (excluding ~~underfrequency load shedding~~ **UFLS** and ~~under voltage load shed~~ **UVLS**) that applies to ~~any transmission facility or electric distribution system~~ **Transmission** where the ~~protection system~~ **Protection System** is subject to one or more requirements in a ~~reliability standard~~ **NERC or Regional Reliability Standard**.

4.2.1.4. Each ~~cranking path~~ **Cranking Path** and group of ~~Elements~~ **elements** meeting the initial switching requirements from a ~~blackstart resource~~ **Blackstart Resource** up to and including the first ~~point of connection~~ **interconnection point** of the starting station service of the next ~~generating unit(s) or aggregated generating facility(ies)~~ **generation unit(s)** to be started.

4.2.2. Responsible Entities listed in 4.1 other than ~~a legal owner of an electric distribution system~~ **Distribution Providers:**

~~all bulk electric system facilities~~ **All BES Facilities.**

4.2.3. Exemptions: The following are exempt from ~~Standard~~ CIP-005-AB-7:

4.2.3.1. ~~Cyber assets~~ **Cyber Assets** at ~~facilities~~ **Facilities** regulated by the Canadian Nuclear Safety Commission.

Alberta Reliability Standard

Cyber Security – Electronic Security

Perimeter(s)

CIP-005-~~AB~~-7



~~4.2.3.2. Cyber assets~~~~Cyber Assets~~ associated with communication networks and data communication links between discrete ~~electronic security perimeters~~~~Electronic Security Perimeters~~.

~~4.2.3.3. [Intentionally left blank.]~~~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3.4. For the legal owner of an electric distribution system~~~~Distribution Providers~~, 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~~~~BES Cyber Systems~~ categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates: ~~See Implementation Plan for Project 2019-03, To be determined in consultation with stakeholders.~~

6. Background:

~~Reliability standard~~~~Standard~~ CIP-005 exists as part of a suite of CIP ~~reliability standards~~~~Standards~~ related to cyber security, which require the initial identification and categorization of ~~BES cyber systems~~~~BES Cyber Systems~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to ~~BES cyber systems~~~~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~~~~BES Cyber Systems~~. For example, a single training program could meet the requirements for training personnel across multiple ~~BES cyber systems~~~~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.”

Alberta Reliability Standard

Cyber Security – Electronic Security

Perimeter(s)

CIP-005-AB-7



Many references in the Applicability section use a threshold of 300 MW for underfrequency load shedding UFLS and under voltage load shed UFLS. This particular threshold of 300 MW for under voltage load shed UFLS and underfrequency load shedding UFLS 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 UFLS and underfrequency load shedding UFLS, which are last ditch efforts to save the Bulk Electric System bulk electric system. A review of underfrequency load shedding UFLS tolerances defined within reliability standards regional reliability standards for underfrequency load shedding UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable underfrequency load shedding UFLS 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 SDF 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 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 BES Cyber Systems with dial-up connectivity Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES cyber systems BES Cyber Systems with external routable connectivity External Routable Connectivity. This also excludes cyber assets Cyber Assets in the BES cyber system BES Cyber System that cannot be directly accessed through external routable connectivity External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES cyber systems 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 BES Cyber Systems located at a control centre Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES cyber systems BES Cyber Systems with dial-up connectivity Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES cyber systems BES Cyber Systems with external routable connectivity External Routable Connectivity. This also excludes cyber assets Cyber Assets in the BES cyber system BES Cyber System that cannot be directly accessed through external routable connectivity External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each protected cyber asset Protected Cyber Asset associated with a referenced high impact BES cyber system BES Cyber System or medium impact BES cyber system BES Cyber System.
- **Electronic Access Points (EAP)** – Applies to electronic access points Electronic Access Points associated with a referenced high impact BES cyber system BES Cyber System or medium

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



impact BES cyber system~~BES-Cyber-System~~.

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

Alberta Reliability Standard

Cyber Security – Electronic Security Perimeter(s)

CIP-005-AB-7



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- <u>AB</u> -7 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES cyber systemsBES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA <p>Medium Impact BES Cyber SystemsBES cyber systems and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA 	<p>All applicable cyber assetsCyber Assets connected to a network via a routable protocol shall reside within a defined electronic security perimeterESP.</p>	<p>An example of evidence may include, but is not limited to, a list of all electronic security perimetersESPs with all uniquely identifiable applicable cyber assetsCyber Assets connected via a routable protocol within each electronic security perimeterESP.</p>

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



CIP-005- AB -7 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems<u>BES cyber systems</u> with <u>external routable connectivity</u> External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> <u>protected cyber assets</u> PCA <p>Medium Impact BES Cyber Systems<u>BES cyber systems</u> with <u>external routable connectivity</u> External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> <u>protected cyber assets</u> PCA 	<p>All <u>external routable connectivity</u> External Routable Connectivity must be through an identified <u>electronic access point</u> Electronic Access Point (EAP).</p>	<p>An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified <u>electronic access points</u> EAPs.</p>
1.3	<p><u>Electronic access points</u> Electronic Access Points for High Impact BES Cyber Systems<u>BES cyber systems</u></p> <p><u>Electronic access points</u> Electronic Access Points for Medium Impact BES Cyber Systems<u>BES cyber systems</u></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>

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



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

Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BES Cyber SystemsBES cyber systems with dial-up connectivitydial-up connectivity and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA <p>Medium Impact BES Cyber SystemsBES cyber systems with dial-up connectivitydial-up connectivity and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA 	<p>Where technically feasible, perform authentication when establishing dial-up connectivitydial-up connectivity with applicable cyber assetsCyber Assets.</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>Electronic access pointsElectronic Access Points for High Impact BES Cyber SystemsBES cyber systems</p> <p>Electronic access pointsElectronic Access Points for Medium Impact BES Cyber SystemsBES cyber systems at control centresControl Centers</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.

Commented AESO: Difference since CIP-005-AB-5:
Removes “Interactive Remote Access” from this statement and adds qualifier in the R2 table instead. Changed name of the R2 table to remove the word “Interactive”.

Original wording:
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.

Commented AESO: Difference since CIP-005-AB-5:
Reworded to include “interactive remote access” qualifier here.

Original wording:
Utilize an **intermediate system** such that the **cyber asset** initiating **interactive remote access** does not directly access an applicable **cyber asset**.

CIP-005- AB -7 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber SystemsBES cyber systems and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA <p>Medium Impact BES Cyber SystemsBES cyber systems with external routable connectivityExternal Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA 	<p>For all interactive remote accessinteractive remote access, utilize an intermediate systemintermediate system such that the cyber assetcyber asset initiating interactive remote accessinteractive remote access does not directly access an applicable cyber assetcyber asset.</p>	<p>Examples of evidence may include, but are not limited to, network diagrams or architecture documents.</p>



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

Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber SystemsBES cyber systems and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA <p>Medium Impact BES Cyber SystemsBES cyber systems with external routable connectivityExternal Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA 	<p>For all interactive remote accessInteractive Remote Access sessions, utilize encryption that terminates at an intermediate systemIntermediate System.</p>	<p>An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.</p>
2.3	<p>High Impact BES Cyber SystemsBES cyber systems and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA <p>Medium Impact BES Cyber SystemsBES cyber systems with external routable connectivityExternal Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA 	<p>Require multi-factor authentication for all interactive remote accessInteractive Remote Access 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"> Something the individual knows such as passwords or PINs. This does not include User ID; Something the individual has such as tokens, digital certificates, or smart cards; or Something the individual is such as fingerprints, iris scans, or other biometric characteristics.



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

Part	Applicable Systems	Requirements	Measures
2.4	<p>High Impact BES Cyber Systems BES cyber systems and their associated:</p> <ul style="list-style-type: none"> protected cyber assets PCA <p>Medium Impact BES Cyber Systems BES cyber systems with external routable connectivity External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> protected cyber assets PCA 	<p>Have one or more methods for determining active vendor remote access sessions (including interactive remote access Interactive Remote Access and system-to-system remote access).</p>	<p>Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including interactive remote access Interactive Remote Access and system-to-system remote access), such as:</p> <ul style="list-style-type: none"> Methods for accessing logged or monitoring information to determine active vendor remote access sessions; 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 Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

Commented AESO: Difference since CIP-005-AB-5:
 New requirement R2.4



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

Part	Applicable Systems	Requirements	Measures
2.5	<p>High Impact BES Cyber SystemsBES cyber systems and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA <p>Medium Impact BES Cyber SystemsBES cyber systems with external routable connectivityExternal Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> protected cyber assetsPCA 	<p>Have one or more method(s) to disable active vendor remote access (including interactive remote accessInteractive Remote Access and system-to-system remote access).</p>	<p>Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including interactive remote accessInteractive Remote Access and system-to-system remote access), such as:</p> <ul style="list-style-type: none"> Methods to disable vendor remote access at the applicable electronic access pointElectronic Access Point for system-to-system remote access; or Methods to disable vendor interactive remote accessInteractive Remote Access at the applicable intermediate systemIntermediate System.

Commented AESO: Difference since CIP-005-AB-5:
 New requirement R2.5

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 SystemsEACMS and Physical Access Control SystemsPACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

Commented AESO: Difference since CIP-005-AB-5:
 New requirement R3

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 <u>Electronic Access Control or Monitoring SystemsEACMS</u> and <u>Physical Access Control SystemsPACS</u>			
Part	Applicable Systems	Requirements	Measures
3.1	<p><u>Electronic access control or monitoring systemsEACMS</u> and <u>physical access control systemsPACS</u> associated with High Impact BES Cyber Systems<u>BES cyber systems</u></p> <p><u>Electronic access control or monitoring systemsEACMS</u> and <u>physical access control systemsPACS</u> associated with Medium Impact BES Cyber Systems<u>BES cyber systems</u> with <u>external routable connectivity</u> External Routable Connectivity</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"> • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.



CIP-005-AB-7 Table R3 – Vendor Remote Access Management for ~~Electronic Access Control or Monitoring SystemsEACMS~~ and ~~Physical Access Control SystemsPACS~~

Part	Applicable Systems	Requirements	Measures
3.2	<p>Electronic access control or monitoring systemsEACMS and physical access control systemsPACS associated with High Impact BES Cyber SystemsBES cyber systems</p> <p>Electronic access control or monitoring systemsEACMS and physical access control systemsPACS associated with Medium Impact BES Cyber SystemsBES cyber systems with external routable connectivity External Routable Connectivity</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.]

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

~~“Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.~~

1.2. Evidence Retention:

~~The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.~~

~~The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.~~

- ~~• Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.~~
- ~~• If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.~~
- ~~• The CEA shall keep the last audit records and all requested and submitted subsequent audit records.~~

1.3. Compliance Monitoring and Enforcement Program:

~~As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.~~

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



Violation Severity Levels

R#	Lower-VSL	Moderate-VSL	High VSL	Severe-VSL
R1			<p>The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)</p>	<p>The Responsible Entity did not document one or more processes for CIP-005-6 Table R1—Electronic Security Perimeter. (R1)</p> <p>OR</p> <p>The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1)</p> <p>OR</p> <p>External Routable Connectivity through the ESP was not through an identified EAP. (1.2)</p> <p>OR</p> <p>The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)</p> <p>OR</p> <p>The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)</p>

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



R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).
R3	The Responsible Entity did not document one or more processes for CIP-005-7 Table R3—Vendor Remote Access Management for EACMS and PACS. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated	The Responsible Entity did not implement any processes for CIP-005-7 Table R3—Vendor Remote Access Management for EACMS and PACS. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

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



R#	Lower-VSL	Moderate-VSL	High-VSL	Severe-VSL
			vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	

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



D. Regional Variances

None.

E. Associated Documents

• [Implementation Plan for Project 2019-03](#)

• CIP-005-7 Technical Rationale

Version History

Version	Effective Date	Action	Description of Change / Tracking
1	4/16/06	R3.2 — Change “Control Center” to “control-center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update

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



Version	Effective Date	Action	Description of Change / Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13 10/1/2022	FERC Order issued approving CIP-005-5.	Initial Version
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	3/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021 <u>TBD</u>	Effective Date	10/1/2022 Modified to address certain directives in FERC Order No. 829 and 850.