Alberta Reliability Standard
Cyber Security – System Security Management
CIP-007-AB-5

A. Introduction

1. Title: Cyber Security – System Security Management

2. Number: CIP-007-AB-5

3. Purpose: To manage system security by specifying select technical, operational, and procedural 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. 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, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R1 – Ports and Services.*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-AB-5 Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • documentation of the need for all enabled ports on all applicable **cyber assets** and **electronic access points**, individually or by group. • listings of the listening ports on the **cyber assets**, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
1.2	High Impact **BES cyber systems** Medium Impact **BES cyber systems** at **control centres**	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either

CIP-007-AB-5 Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
		media.	logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R2 – Security Patch Management.*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-AB-5 Table R2 – Security Patch Management			
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**	A patch management process for tracking, evaluating, and installing cyber security patches for applicable **cyber assets**. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable **cyber assets** that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual **BES cyber system** or **cyber asset** basis.
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**	At least once every 35 **days**, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 **days**.

CIP-007-AB-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	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**		
2.3	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**	For applicable patches identified in part 2.2, within 35 **days** of the evaluation completion, take one of the following actions: • apply the applicable patches; or • create a dated mitigation plan; or • revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of **BES cyber system** component software revision, or registry exports that show software has been installed); or • a dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.
2.4	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and	For each mitigation plan created or revised in part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in part 2.3 is approved by the **CIP senior**	An example of evidence may include, but is not limited to, records of implementation of mitigations.

CIP-007-AB-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	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**	**manager** or delegate.	

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R3 – Malicious Code Prevention.*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-AB-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	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**	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High Impact **BES cyber systems** and their associated:	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to:

CIP-007-AB-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	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**		• records of response processes for malicious code detection • records of the performance of these processes when malicious code is detected.
3.3	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**	For those methods identified in part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R4 – Security Event Monitoring.*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-AB-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	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**	Log events at the **BES cyber system** level (per **BES cyber system** capability) or at the **cyber asset** level (per **cyber asset** capability) for identification of, and after-the-fact investigations of, **cyber security incidents** that includes, as a minimum, each of the following types of events: 4.1.1. detected successful login attempts; 4.1.2. detected failed access attempts and failed login attempts; 4.1.3. detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the **BES cyber system** is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per **cyber asset** or **BES cyber system** capability): 4.2.1. detected malicious code from part 4.1; and 4.2.2. detected failure of part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.
4.3	High Impact **BES cyber systems** and their associated:	Where technically feasible, retain applicable event logs identified in part 4.1 for at least	Examples of evidence may include, but are not limited to, documentation of the event log

CIP-007-AB-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** at **control centres** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	the last 90 consecutive **days** except under **CIP exceptional circumstances**.	retention process and paper or system generated reports showing log retention configuration set at 90 **days** or greater.
4.4	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 **days** to identify undetected **cyber security incidents**.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R5 – System Access Controls.*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts *in CIP-007-AB-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-AB-5 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control**	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-AB-5 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems; and 3. **protected cyber assets** Medium Impact **BES cyber systems** at **control centres** 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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**		
5.2	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**	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the **BES cyber system**.

CIP-007-AB-5 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.
5.4	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**	Change known default passwords, per **cyber asset** capability.	Examples of evidence may include, but are not limited to: • records of a procedure that passwords are changed when new devices are in production; or • documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**;	For password-only authentication for interactive user access, either technically or procedurally enforce the following password	Examples of evidence may include, but are not limited to: • system-generated reports or screen-shots of the

CIP-007-AB-5 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	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**	parameters: 5.5.1. password length that is, at least, the lesser of eight characters or the maximum length supported by the **cyber asset**; and 5.5.2. minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the **cyber asset**.	system enforced password parameters, including length and complexity; or • attestations that include a reference to the documented procedures that were followed.
5.6	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 **months**.	Examples of evidence may include, but are not limited to: • system-generated reports or screen-shots of the system enforced periodicity of changing passwords; or • attestations that include a reference to the documented procedures that were followed.
5.7	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control**	Where technically feasible, either: • limit the number of unsuccessful authentication attempts; or	Examples of evidence may include, but are not limited to: • documentation of the account-lockout parameters; or

CIP-007-AB-5 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems; and 3. **protected cyber assets** Medium Impact **BES cyber systems** at **control centres** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	• generate alerts after a threshold of unsuccessful authentication attempts.	• rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

Revision History

Date	Description
2017-10-01	Initial release.