Alberta Reliability Standard
Cyber Security – Physical Security of BES Cyber Systems
CIP-006-AB-5

A. Introduction

1. Title: Cyber Security – Physical Security of BES Cyber Systems

2. Number: CIP-006-AB-5

3. Purpose: To manage physical access to **BES cyber systems** by specifying a physical security plan 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 physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan.*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-AB-5 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact **BES cyber systems** without **external routable connectivity** **Physical access control systems** associated with: • High Impact **BES cyber systems**, or • Medium Impact **BES cyber systems** with **external routable connectivity**	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.
1.2	Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Utilize at least one physical access control to allow unescorted physical access into each applicable **physical security perimeter** to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each **physical security perimeter** and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-AB-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into **physical security perimeters** to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the **physical security perimeters** and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.4	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Monitor for unauthorized access through a physical access point into a **physical security perimeter**.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a **physical security perimeter**.
1.5	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated:	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a **physical security perimeter** to the personnel identified in the **bulk electric system cyber security incident** response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a **physical security perimeter** and additional evidence that the alarm or alert was issued and communicated as

CIP-006-AB-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**		identified in the **bulk electric system cyber security incident** response plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	**Physical access control systems** associated with: • High Impact **BES cyber systems**, or • Medium Impact **BES cyber systems** with **external routable connectivity**	Monitor each **physical access control system** for unauthorized physical access to a **physical access control system**.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a **physical access control system**.
1.7	**Physical access control systems** associated with: • High Impact **BES cyber systems**, or • Medium Impact **BES cyber systems** with **external routable connectivity**	Issue an alarm or alert in response to detected unauthorized physical access to a **physical access control system** to the personnel identified in the **bulk electric system cyber security incident** response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to **physical access control systems** and additional evidence that the alarm or alerts was issued and communicated as identified in the **bulk electric system cyber security incident** response plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
1.8	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of

CIP-006-AB-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. **protected cyber assets** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	into each **physical security perimeter**, with information to identify the individual and date and time of entry.	physical entry into each **physical security perimeter** and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into **physical security perimeters** that show the individual and the date and time of entry into **physical security perimeter**.
1.9	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Retain physical access logs of entry of individuals with authorized unescorted physical access into each **physical security perimeter** for at least ninety **days**.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into **physical security perimeters** that show the date and time of entry into **physical security perimeter**.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-AB-5 Table R2 – Visitor Control Program.*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-AB-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-AB-5 Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each **physical security perimeter**, except during **CIP exceptional circumstances**.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within **physical security perimeters** and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Require manual or automated logging of visitor entry into and exit from the **physical security perimeter** that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during **CIP exceptional circumstances**.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within **physical security perimeters** and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets** Medium Impact **BES cyber systems** with **external routable connectivity** and	Retain visitor logs for at least ninety **days**.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety **days**.

CIP-006-AB-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**		

R3. Each Responsible Entity shall implement one or more documented **physical access control system** maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-AB-5 Table R3 – Maintenance and Testing Program.*

M3. Evidence must include each of the documented **physical access control system** maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-AB-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-AB-5 Table R3 – Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	**Physical access control systems** associated with: • High Impact **BES cyber systems**, or • Medium Impact **BES cyber systems** with **external routable connectivity** Locally mounted hardware or devices at the **physical security perimeter** associated with: • High Impact **BES cyber systems**, or • Medium Impact **BES cyber systems** with **external routable connectivity**	Maintenance and testing of each **physical access control system** and locally mounted hardware or devices at the **physical security perimeter** at least once every 24 **months** to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each **physical access control system** and locally mounted hardware or devices associated with each applicable **physical security perimeter** at least once every 24 **months** and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 **months**.

Revision History

Date	Description
2017-10-01	Initial release.