Alberta Reliability Standard
Cyber Security – Recovery Plans for BES Cyber Systems
CIP-009-AB-5

A. Introduction

1. Title: Cyber Security – Recovery Plans for BES Cyber Systems

2. Number: CIP-009-AB-5

3. Purpose: To recover reliability functions performed by **BES cyber systems** by specifying recovery plan requirements in support of the continued stability, operability, and reliability of 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**;

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 have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-AB-5 Table R1 – Recovery Plan Specifications.*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-AB-5 Table R1 – Recovery Plan Specifications.*

CIP-009-AB-5 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control**	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-AB-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems		
1.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	One or more processes for the backup and storage of information required to recover **BES cyber system** functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover **BES cyber system** functionality.
1.4	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** at **control centres** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	One or more processes to preserve data, per **cyber asset** capability, for determining the cause of a **cyber security incident** that triggers activation of the recovery plan(s). Data preservation should not	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

CIP-009-AB-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	impede or restrict recovery.	

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing.*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** at **control centres** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	Test each of the recovery plans referenced in requirement R1 at least once every 15 **months**: • by recovering from an actual incident; • with a paper drill or tabletop exercise; or • with an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 **months**. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and	Test a representative sample of information used to recover **BES cyber system** functionality at least once every 15 **months** to ensure that the information is useable	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents)

CIP-009-AB-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. **physical access control systems** Medium Impact **BES cyber systems** at **control centres** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	and is compatible with current configurations. An actual recovery that incorporates the information used to recover **BES cyber system** functionality substitutes for this test.	and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact **BES cyber systems**	Test each of the recovery plans referenced in requirement R1 at least once every 36 **months** through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • an operational exercise at least once every 36 **months** between exercises, that demonstrates recovery in a representative environment; or • an actual recovery response that occurred within the 36 **month** timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication.*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring**	No later than 90 **days** after completion of a recovery plan test or actual recovery: 3.1.1. document any lessons	An example of evidence may include, but is not limited to, all of the following: 1. dated documentation of

CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems; and 2. **physical access control systems** Medium Impact **BES cyber systems** at **control centres** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. dated and revised recovery plan showing any changes based on the lessons learned; and 3. evidence of plan update distribution including, but not limited to: • emails; • USPS or other mail service; • electronic distribution system; or • training sign-in sheets.
3.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** at **control centres** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	No later than 60 **days** after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. update the recovery plan; and 3.2.2. notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. evidence of plan update distribution including, but not limited to: • emails; • USPS or other mail service; • electronic distribution system; or

CIP-009-AB-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• training sign-in sheets.

Revision History

Date	Description
2017-10-01	Initial release.