Alberta Reliability Standard
Cyber Security – Incident Reporting and Response Planning
CIP-008-AB-5

A. Introduction

1. Title: Cyber Security – Incident Reporting and Response Planning

2. Number: CIP-008-AB-5

3. Purpose: To mitigate the risk to the reliable operation of the **bulk electric system** as the result of a **cyber security incident** by specifying incident response requirements.

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 document one or more **cyber security incident** response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications.*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications.*

CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	One or more processes to identify, classify, and respond to **cyber security incidents**.	An example of evidence may include, but is not limited to, dated documentation of **cyber security incidents** response plan(s) that include the process to identify, classify, and respond to **cyber security incidents**.
1.2	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	One or more processes to determine if an identified **cyber security incident** is a **reportable cyber security incident** and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a **reportable cyber security incident**.	Examples of evidence may include, but are not limited to, dated documentation of **cyber security incident** response plan(s) that provide guidance or thresholds for determining which **cyber security incidents** are also **reportable cyber security incidents** and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).
1.3	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	The roles and responsibilities of **cyber security incident** response groups or individuals.	An example of evidence may include, but is not limited to, dated **cyber security incident** response process(es) or procedure(s) that define roles and responsibilities (e.g.,

CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
			monitoring, reporting, initiating, documenting, etc.) of **cyber security incident** response groups or individuals.
1.4	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	Incident handling procedures for **cyber security incidents**.	An example of evidence may include, but is not limited to, dated for **cyber security incident** response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented **cyber security incident** response plans to collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R2 – Cyber Security Incident Response 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-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*

CIP-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	Test each **cyber security incident** response plan(s) at least once every 15 **months**: • by responding to an actual **reportable cyber security incident**; • with a paper drill or tabletop exercise of a **reportable cyber security incident**; or • with an operational exercise of a **reportable cyber security incident**.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High Impact **BES cyber systems** Medium Impact **BES cyber**	Use the **cyber security incident** response plan(s) under Requirement R1 when responding to a **reportable**	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the

CIP-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems	**cyber security incident** or performing an exercise of a **reportable cyber security incident**. Document deviations from the plan(s) taken during the response to the incident or exercise.	incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	Retain records related to **reportable cyber security incident**.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to **reportable cyber security incidents**.

R3. Each Responsible Entity shall maintain each of its **cyber security incident** response plans according to each of the applicable requirement parts in *CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each **cyber security incident** response plan according to the applicable requirement parts in *CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	No later than 90 **days** after completion of a **cyber security incident** response plan(s) test or actual **reportable cyber security incident** response: 3.1.1. document any lessons learned or document the absence of any lessons learned; 3.1.2. update the **cyber**	An example of evidence may include, but is not limited to, all of the following: 1. dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the **cyber security incident** response plan(s) test or actual **reportable cyber security incident**

CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
		security incident response 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 **cyber security incident** response plan of the updates to the **cyber security incident** response plan based on any documented lessons learned.	response or dated documentation stating there were no lessons learned; 2. dated and revised **cyber security incident** response 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** Medium Impact **BES cyber systems**	No later than 60 **days** after a change to the roles or responsibilities, **cyber security incident** response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. update the **cyber security incident** response plan(s); and 3.2.2. notify each person or group with a defined role in the **cyber security incident** response plan of the updates.	An example of evidence may include, but is not limited to: 1. dated and revised **cyber security incident** response 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 • training sign-in sheets.

Revision History

Date	Description
2017-10-01	Initial release.