Alberta Reliability Standard
Cyber Security – Configuration Change Management and Vulnerability Assessments
CIP-010-AB-1

A. Introduction

1. Title: Cyber Security – Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-AB-1

3. Purpose: To prevent and detect unauthorized changes to **BES cyber systems** by specifying configuration change management and vulnerability assessment requirements in support of protecting **BES cyber systems** from 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-010-AB-1 Table R1 – Configuration Change Management*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-AB-1 Table R1 – Configuration Change Management

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** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. any commercially available or open-source application software (including version) intentionally installed; 1.1.3. any custom software installed; 1.1.4. any logical network accessible ports; and 1.1.5. any security patches applied.	Examples of evidence may include, but are not limited to: • a spreadsheet identifying the required items of the baseline configuration for each **cyber asset**, individually or by group; or • a record in an asset management system that identifies the required items of the baseline configuration for each **cyber asset**, individually or by group.
1.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • a change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a

CIP-010-AB-1 Table R1 – Configuration Change 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**		change management system for each change; or • documentation that the change was performed in accordance with the requirement.
1.3	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 a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 **days** of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 **days** of the date of the completion of the change.
1.4	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:	For a change that deviates from the existing baseline configuration: 1.4.1. prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. following the change, verify that required cyber security controls determined	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-AB-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets**	in 1.4.1 are not adversely affected; and 1.4.3. document the results of the verification.	
1.5	High Impact **BES cyber systems**	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

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-010-AB-1 Table R2 – Configuration Monitoring*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R2 – Configuration*

Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-AB-1 Table R2 – Configuration Monitoring			
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**	Monitor at least once every 35 **days** for changes to the baseline configuration (as described in requirement R1, part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R3– Vulnerability Assessments*.

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-AB-1 Table R3 – Vulnerability Assessments			
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**	At least once every 15 **months**, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • a document listing the date of the assessment (performed at least once every 15 **months**), the controls assessed for each **BES cyber system** along with the method of assessment; or • a document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-AB-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact **BES cyber systems**	Where technically feasible, at least once every 36 **months**: 3.2.1 perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the **BES cyber system** in a production environment; and 3.2.2 document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 **months**), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
3.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **protected cyber assets**	Prior to adding a new applicable **cyber asset** to a production environment, perform an active vulnerability assessment of the new **cyber asset**, except for **CIP exceptional circumstances** and like replacements of the same type of **cyber asset** with a baseline configuration that models an existing baseline configuration of the previous or other existing **cyber asset**.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new **cyber asset**) and the output of any tools used to perform the assessment.
3.4	High Impact **BES cyber systems** and their associated: 1. **electronic access**	Document the results of the assessments conducted according to parts 3.1, 3.2, and 3.3 and the action plan to	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a

CIP-010-AB-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
	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**	remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Revision History

Date	Description
2017-10-01	Initial release.