Alberta Reliability Standard
Cyber Security – Personnel & Training
CIP-004-AB-5.1

A. Introduction

1. Title: Cyber Security – Personnel & Training

2. Number: CIP-004-AB-5.1

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the **bulk electric system** from individuals accessing **BES cyber systems** by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting **BES cyber systems**.

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 one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R1 – Security Awareness Program.*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-AB-5.1 Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High Impact **BES cyber systems** Medium Impact **BES cyber systems**	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to **BES cyber systems**.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-AB-*

5.1 Table R2 – Cyber Security Training Program.

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-AB-5.1 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-AB-5.1 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Training content on: 2.1.1. cyber security policies; 2.1.2. physical access controls; 2.1.3. electronic access controls; 2.1.4. the visitor control program; 2.1.5. handling of **BES cyber system information** and its storage; 2.1.6. identification of a **cyber security incident** and initial notifications in accordance with the entity's incident response plan; 2.1.7. recovery plans for **BES cyber systems**; 2.1.8. response to **cyber security incidents**; and 2.1.9. cyber security risks associated with a **BES cyber system**'s electronic interconnectivity and interoperability with other **cyber assets**.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.
2.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and	Require completion of the training specified in part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable	Examples of evidence may include, but are not limited to, training records and documentation of when **CIP exceptional circumstances** were invoked.

CIP-004-AB-5.1 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	**cyber assets**, except during **CIP exceptional circumstances**.	
2.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Require completion of the training specified in part 2.1 at least once every 15 **months**.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to **BES Cyber Systems** that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program.*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive **months** or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.
3.5	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals

CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	assessment completed according to parts 3.1 to 3.4 within the last seven years.	with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R4 – Access Management Program.*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-AB-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and	Process to authorize based on need, as determined by the Responsible Entity, except for **CIP exceptional circumstances**: 4.1.1. electronic access; 4.1.2. unescorted physical access into a **physical security perimeter**; and 4.1.3. access to designated storage locations, whether physical or electronic, for **BES cyber system information**.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a **physical security perimeter**, and access to designated storage locations, whether physical or electronic, for **BES cyber system information**.

CIP-004-AB-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. **physical access control systems**.		
4.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control**	For electronic access, verify at least once every 15 **months** that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. a dated listing of all accounts/account groups or roles within the system; 2. a summary description of privileges associated with each group or role; 3. accounts assigned to the group or role; and 4. dated evidence showing verification of the privileges for the group are

CIP-004-AB-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems.		authorized and appropriate to the work function performed by people assigned to each account.
4.4	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	Verify at least once every 15 **months** that access to the designated storage locations for **BES cyber system information**, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. a dated listing of authorizations for **BES cyber system information**; 2. any privileges associated with the authorizations; and 3. dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R5 – Access Revocation.*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-AB-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and	A process to initiate removal of an individual's ability for unescorted physical access and **interactive remote access** upon a termination action, and complete the	An example of evidence may include, but is not limited to, documentation of all of the following: 1. dated workflow or sign-off

CIP-004-AB-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	form verifying access removal associated with the termination action; and 2. logs or other demonstration showing such persons no longer have access.
5.2	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next **day** following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. dated workflow or sign-off form showing a review of logical and physical access; and 2. logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact **BES cyber systems** and their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**. Medium Impact **BES cyber systems** with **external routable connectivity** and	For termination actions, revoke the individual's access to the designated storage locations for **BES cyber system information**, whether physical or electronic (unless already revoked according to requirement R5.1), by the end of the next **day** following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or signoff form verifying access removal to designated physical areas or cyber systems containing **BES cyber system information** associated with the terminations and dated within the next **day** of the termination action.

CIP-004-AB-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	their associated: 1. **electronic access control and monitoring systems**; and 2. **physical access control systems**.		
5.4	High Impact **BES cyber systems** and their associated: • **electronic access control and monitoring systems**.	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to parts 5.1 or 5.3) within 30 **days** of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or signoff form showing access removal for any individual **BES cyber assets** and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.5	High Impact **BES cyber systems** and their associated: • **electronic access control and monitoring systems**.	For termination actions, change passwords for shared account(s) known to the user within 30 **days** of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 **days** following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 **days** following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • workflow or sign-off form showing password reset within 30 **days** of the termination; • workflow or sign-off form showing password reset within 30 **days** of the reassignments or transfers; or • documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 **days** following the end of the operating circumstance.

Revision History

Date	Description
2017-10-01	Initial release.