Alberta Reliability Standard
Cyber Security – Personnel and Training
CIP-004-AB-7

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-AB-7

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, security awareness, and access management in support of protecting **BES cyber systems**.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this **reliability standard** where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional 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 Responsible Entity, 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 an **electric distribution system** 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 **blackstart resource** up to and including the first **point of connection** of the starting station service of the next **generating unit**(s) or **aggregated generating facility**(ies) to be started.

4.1.3. the **operator** of a **generating unit** that is part of the **bulk electric system** and the **operator** of an **aggregated generating facility** that is part of the **bulk electric system**;

4.1.4. the **legal owner** of a **generating unit** that is part of the **bulk electric system** and the **legal owner** of an **aggregated generating facility** that is part of the **bulk electric system**;

4.1.5. [Intentionally left blank.]

4.1.6. the **operator** of a **transmission facility**

4.1.7. the **legal owner** of a **transmission facility**; and

4.1.8. the **ISO**

4.2. Facilities: For the purpose of the requirements contained herein, the following facilities, systems, and equipment owned by each Responsible Entity in 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. Legal owner of an **electric distribution system** and **legal owner** of a **transmission facility:** 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 the Responsible Entity, 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 facility** or **electric distribution system** 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 **blackstart resource** up to and including the first **point of connection** of the starting station service of the next **generating unit**(s) or **aggregated generating facility**(ies) to be started.

4.2.2. Responsible Entities listed in 4.1 other than a **legal owner** of an **electric distribution system:** all **bulk electric system** facilities.

4.2.3. Exemptions: The following are exempt from **reliability standard** CIP-004-AB-7

4.2.3.1. cyber assets at facilities regulated by the Canadian Nuclear Safety Commission.

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 section 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 identification and categorization processes.

5. Effective Dates**:** See CIP-PLAN-AB-3, *Cyber Security Implementation Plan for CIP Cyber Security Reliability Standards*

6. Background**: Reliability standard** CIP-004 exists as part of a suite of CIP **reliability standards** related to cyber security, which require the initial identification and categorization of **BES cyber systems**

and require a minimum level of organizational, operational, and procedural controls to mitigate risk to **BES cyber systems.**

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the **reliability standards** include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security **reliability standards** could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the **reliability standards**.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact **BES cyber systems**. For example, a single training program could meet the requirements for training personnel across multiple **BES cyber systems**.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the **reliability standards**, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for **underfrequency load shedding** and **under voltage load shed**. This particular threshold of 300 MW for **under voltage load shed** and **underfrequency load shedding** was provided in Version 1 of the NERC CIP Cyber Security **reliability standards**. The threshold remains at 300 MW since it is specifically addressing **under voltage load shed** and **underfrequency load shedding**, which are last ditch efforts to save the **bulk electric system**. A review of **underfrequency load shedding** tolerances defined within **reliability standards** for **underfrequency load shedding** program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable **underfrequency load shedding** operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- High Impact **BES Cyber Systems** – Applies to **BES cyber systems** categorized as high impact according to the CIP-002-AB-5.1 and any amendments made thereto from time to time identification and categorization processes.

- Medium Impact **BES Cyber Systems** – Applies to **BES cyber systems** categorized as medium impact according to the CIP-002-AB-5.1 and any amendments made thereto from time to time identification and categorization processes.

- Medium Impact **BES Cyber Systems** with **External Routable Connectivity** – Only applies to medium impact **BES cyber systems** with **external routable connectivity**. This also excludes **cyber assets** in the **BES cyber system** that cannot be directly accessed through **external routable connectivity**.

- **Electronic Access Control or Monitoring Systems** – Applies to each **electronic access control or monitoring system** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems** – Applies to each **physical access control system** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**.

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-7 Table R1 – Security Awareness Program*. *[Alberta Risk Rating: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-AB-7 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 one or more 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-7 Table R2 – Cyber Security Training Program*. [*Alberta Risk Rating*: *Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-AB-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-AB-7 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 or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or 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 incident**; and 2.1.9. Cyber security risks associated with a **BES cyber system's** electronic interconnectivity and interoperability with other **cyber assets**, including **transient cyber assets**, and with **removable media**.	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.

CIP-004-AB-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable **cyber assets**, except during **CIP exceptional circumstances**.	Examples of evidence may include, but are not limited to, training records and documentation of when **CIP exceptional circumstances** were invoked.
2.3	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** with **external routable connectivity** and their associated: 1. **electronic access control**	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.

CIP-004-AB-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	or monitoring systems; and 2. **physical access control systems**		

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) 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-7 Table R3 – Personnel Risk Assessment Program*. *[Alberta Risk Rating: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-AB-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-AB-7 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 or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or 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 or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** with **external routable**	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	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-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	connectivity and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	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.	
3.3	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** with **external routable connectivity** and their associated: 1. **electronic access control or 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 or 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.

CIP-004-AB-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**		
3.5	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems;** and 2. **physical access control systems**	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals 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 one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-AB-7 Table R4 – Access Management Program. [Alberta Risk Rating: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP- 004-AB-7 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-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	Process to authorize based on need, as determined by the Responsible Entity, except for **CIP exceptional circumstances**: 4.1.1 Electronic access; and 4.1.2 Unescorted physical access into a **physical security perimeter**	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a **physical security perimeter**.
4.2	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring**	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

CIP-004-AB-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems; and 2. **physical access control systems**		shared account listing).
4.3	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	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 authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-AB-7 Table R5 – Access Revocation. [Alberta Risk Rating: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-AB-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-AB-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	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 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).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off 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 or monitoring systems**; and 2. **physical access control**	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	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

CIP-004-AB-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	systems Medium Impact **BES cyber systems** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	that the individual no longer requires retention of that access.	such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact **BES cyber systems** and their associated: • **electronic access control or monitoring systems**	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 **days** of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual **cyber assets** and software applications as determined necessary to completing the revocation of access and dated within thirty **days** of the termination actions
5.4	High Impact **BES cyber systems** and their associated: • **electronic access control or 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**	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.

CIP-004-AB-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
		following the end of the operating circumstances.	

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to **BES cyber system information** pertaining to the "Applicable Systems" identified in *CIP-004-AB-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP- 004-AB-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to **BES cyber system information** in the context of this requirement, an individual has both the ability to obtain and use **BES cyber system information.** Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access **BES cyber system information** (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Alberta Risk Rating: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-AB-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-AB-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	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** with **external routable connectivity** and their associated: 1. **electronic**	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for **CIP exceptional circumstances**: 6.1.1. Provisioned electronic access to electronic **BES cyber system information**; and 6.1.2. Provisioned physical access to physical **BES cyber system information**.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-AB-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
	access control or monitoring systems; and 2. **physical access control systems**		
6.2	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	Verify at least once every 15 **months** that all individuals with provisioned access to **BES cyber system information**: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

CIP-004-AB-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.3	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** with **external routable connectivity** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems**	For termination actions, remove the individual's ability to use provisioned access to **BES cyber system information** (unless already revoked according to Part 5.1) by the end of the next **day** following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next **day** of the termination action.

C. Compliance

[Intentionally left blank.]

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

- CIP-PLAN-AB-3, *Cyber Security – Implementation Plan for CIP Cyber Security Reliability Standards* and any amendments made thereto from time to time.
- AESO Information Document, #2015-003RS, *Guidance Information for CIP Standards* and any amendments made thereto from time to time.

Version History

Version	Effective Date	Description of Changes
5	Oct 1, 2017	Initial Version
7	April 1, 2026	Addressed FERC directives from Order No. 791. Revised to enhance BES reliability for entities to manage their BCSI.