## Standard Development Timeline

*This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.*

### Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

### Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

| Anticipated Actions | Anticipated Date |
|---|---|
| 45-day Formal Comment Period with Parallel Initial Ballot | 11/03/2011 |
| 30-day Formal Comment Period with Parallel Successive Ballot | March 2012 |
| Recirculation ballot | June 2012 |
| BOT adoption | June 2012 |

## Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]

2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

## Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | 1/16/06 | R3.2 — Change "Control Center" to "control center" | 3/24/06 |
| 2 | 9/30/09 | Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | 12/16/09 | Updated version number from -2 to -3<br>Approved by the NERC Board of Trustees | |
| 3 | 3/31/10 | Approved by FERC | |
| 4 | 12/30/10 | Modified to add specific criteria for Critical Asset identification | Update |
| 4 | 1/24/11 | Approved by the NERC Board of Trustees | Update |
| 5 | TBD | Modified to coordinate with other CIP standards and to revise format to use RBS Template | |

## Definitions of Terms Used in the Standard

*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*

*When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.*

## A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** Standard CIP-004-5 requires that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Assets and BES Cyber Systems, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

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 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 **Balancing Authority**

4.1.2 **Distribution Provider** that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
- A Transmission Protection System required by a NERC or regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 **Interchange Coordinator**

4.1.6 **Load-Serving Entity** that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard

4.1.7 **NERC**

**4.1.8 Regional Entity**

**4.1.9 Reliability Coordinator**

**4.1.10 Transmission Operator**

**4.1.11 Transmission Owner**

**4.2. Facilities:**

**4.2.1 Load Serving Entity:** One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard

**4.2.2 Distribution Providers**: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
- A Transmission Protection System required by a NERC or regional Reliability Standard
- Its Transmission Operator's restoration plan

**4.2.3 All other Responsible Entities**: **All BES Facilities**

**4.2.4 Exemptions:** The following are exempt from Standard CIP-004-5:

**4.2.4.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

**4.2.4.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

**4.2.4.3** In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

**4.2.4.4** Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

## 5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

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 specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

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 infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they 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 Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security 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 Standards.

**Applicability**

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the 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 applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. 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.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 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.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

## B. Requirements and Measures

**Rationale for R1:** Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices.

**Summary of Changes:** Reformatted into table structure.

**R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-004-5 Table R1 – Security Awareness Program | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 1.1 | All  Responsible Entities | A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis. | Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed. |
| **Reference to prior version:**<br>*CIP-004-4 R1* | | **Change Rationale:** *Changed to remove the need to ensure everyone with authorized access receives this awareness. Moved example mechanisms to guidance.* | |

**Rationale for R2:** To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems contains the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

**Summary of Changes:**

1. Addition of specific role training for

- the visitor control program;
- electronic interconnectivity supporting the operation and control of BES Cyber Systems
- storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems

**R2.** Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

**M2.** Evidence must include the training program that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*.

| **CIP-004-5 Table R2 – Cyber Security Training Program** | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 2.1 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | Define the roles that require training. | Acceptable evidence must include a list of roles and what training is needed for each role. |
| **Reference to prior version:** NEW | | **Change Rationale:** *The first thing needed in a role based training program is to understand what roles your people have to help plan what training modules you need to provide.* | |

<table>
<tr><th colspan="4">CIP-004-5 Table R2 – Cyber Security Training Program</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>2.2</td><td>High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems</td><td>Training on the security controls protecting the Responsible Entity’s BES Cyber Systems.</td><td>Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b><br><i>CIP004-4 R2.2.1</i></td><td colspan="2"><b>Change Rationale:</b> <i>Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.</i></td></tr>
<tr><td>2.3</td><td>High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems</td><td>Training on the proper use of physical access controls protecting the Responsible Entity’s BES Cyber Systems.</td><td>Evidence may include, but is not limited to, training material on the proper use of physical access controls for BES Cyber Systems.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b><br><i>CIP004-4 R2.2.2</i></td><td colspan="2"><b>Change Rationale:</b> <i>Minor wording changes.</i></td></tr>
<tr><td>2.4</td><td>High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems</td><td>Training on the electronic access controls protecting the Responsible Entity’s BES Cyber Systems.</td><td>Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b><br><i>CIP004-4 R2.2.2</i></td><td colspan="2"><b>Change Rationale:</b> <i>Minor wording changes.</i></td></tr>
<tr><td>2.5</td><td>High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems</td><td>Training on the visitor control program.</td><td>Evidence may include, but is not limited to, training material on the visitor control program.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b><br><i>NEW</i></td><td colspan="2"><b>Change Rationale:</b> <i>Personnel administering the <b>visitor control program</b> and/or providing escort should be part of the core training; FERC Order 706 - paragraph 432.</i></td></tr>
</table>

| CIP-004-5 Table R2 – Cyber Security Training Program | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 2.6 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | Training on handling of BES Cyber System Information and storage media. | Evidence may include, but is not limited to, training material on the handling of BES Cyber System Information, including storage media. |
| **Reference to prior version:**<br>*CIP004-4 R2.2.3* | | **Change Rationale:** *Core training on the* ***handling of BES Cyber System (****not Critical Cyber Assets****) Information****, with the addition of* ***storage media;*** *FERC Order 706 -paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16)* | |
| 2.7 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | Training on identification of a potential BES Cyber Security Incident and associated notifications. | Evidence may include, but is not limited to, training material on the identification of a potential BES Cyber Security Incident and associated notifications. |
| **Reference to prior version:**<br>*CIP004-4 R2.2.4 (new; implied but not stated in CIP-004 or CIP-008)* | | **Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order 706 - paragraph 413; Related to CIP-008 & DHS Incident Reporting requirements for those with roles in incident reporting.* | |
| 2.8 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | Training on recovery plans for BES Cyber Systems. | Evidence may include, but is not limited to, training material on recovery plans for BES Cyber Systems. |
| **Reference to prior version:**<br>*CIP004-4 R2.2.4* | | **Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order 706 - paragraph 413.* | |

| **CIP-004-5 Table R2 – Cyber Security Training Program** | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 2.9 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | Training on response to BES Cyber Security Incidents. | Evidence may include, but is not limited to, training material on the response to a BES Cyber Security Incident. |
| **Reference to prior version:**<br>*CIP004-4 R2.2.4* | | **Change Rationale:** *Minor wording changes.* | |
| 2.10 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets. | Evidence may include, but is not limited to, training material on the electronic interconnectivity and interoperability with other Cyber Assets. |
| **Reference to prior version:**<br>*NEW* | | **Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order 706 - paragraph 434.* | |

**Rationale for R3:** To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

**Summary of Changes:** Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

**R3.** Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

**M3.** Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

| CIP-004-5 Table R3 – Cyber Security Training | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 3.1 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances. | Evidence may include, but is not limited to, for each individual requiring access, dated individual training records, the date access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked. |
| **Reference to prior version:**<br>*CIP004-4 R2.1* | | **Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order 706 - paragraph 431 is detailed in CIP-003-5..* | |

<table>
<tr><th colspan="4">CIP-004-5 Table R3 – Cyber Security Training</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>3.2</td><td>High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets</td><td>Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.</td><td>Evidence may include, but is not limited to, dated individual training records.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b><br><i>CIP004-4 R2.3</i></td><td colspan="2"><b>Change Rationale:</b> <i>Updated to further define what “Annual” training means.</i></td></tr>
</table>

**Rationale for R4:** To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.

**Summary of Changes:** Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

**R4.** Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

**M4.** Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.

| CIP-004-5 Table R4 – Personnel Risk Assessment Program | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 4.1 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | An initial personnel risk assessment that includes identity verification. | Acceptable evidence must include the documented risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification. |
| **Reference to prior version:**<br>*CIP004-4 R3.1* | | **Change Rationale:** *Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment.* | |

| CIP-004-5 Table R4 – Personnel Risk Assessment Program | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 4.2 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems | Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six 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. | Acceptable evidence must include the documented risk assessment program with a requirement for a seven year criminal history record check in accordance with Requirement R4, Part 4.2. |
| **Reference to prior version:**<br>*CIP004-4 R3.1* | | **Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.* | |

<table>
<tr><th colspan="4">CIP-004-5 Table R4 – Personnel Risk Assessment Program</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>4.3</td><td>High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems</td><td>Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.</td><td>Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.3.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b><br><i>NEW</i></td><td colspan="2"><b>Change Rationale:</b> <i>There should be documented criteria or a process used to evaluate personnel risk assessments.</i></td></tr>
<tr><td>4.4</td><td>High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems</td><td>Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.</td><td>Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.4.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b><br><i>CIP-004-4 R3.3</i></td><td colspan="2"><b>Change Rationale:</b> <i>Separated into its own table item.</i></td></tr>
</table>

**Rationale for R5:** To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

**R5.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment.[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

**M5.** Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

| **CIP-004-5 Table R5 – Personnel Risk Assessment** | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirement** | **Measures** |
| 5.1 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances. | Evidence may include, but is not limited to:<br>• Dated records showing that personnel risk assessments were completed before access was authorized;<br>• Dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5 R4 before access was authorized. |
| **Reference to prior version:**<br>*CIP-004-3 R3, R3.3* | | **Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.* | |

| CIP-004-5 Table R5 – Personnel Risk Assessment | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirement** | **Measures** |
| 5.2 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | Update each personnel risk assessment at least once every seven calendar years after the initial personnel risk assessment. | Evidence may include, but is not limited to, current and former personnel risk assessment records. |
| **Reference to prior version:**<br>*CIP-004-4 R3.2* | | **Change Rationale:** *Eliminated the "for cause" renewal.* | |

**Rationale for R6:** To ensure that individuals with access to BES Cyber Systems have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and part of the delegations referenced in CIP-003-5.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in 6.4 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

**Summary of Changes:** The primary change here involves pulling the access management requirements from CIP-003-4, CIP-004-4 and CIP-007-4 into a single requirement. The requirements from version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

**R6.** Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]*

**M6.** Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – 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-004-5 Table R6 – Access Management Program** | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 6.1 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. | Evidence may include, but is not limited to:<br>(i) a system-generated list of people with electronic access and a sampling of accounts to verify unauthorized users do not have access,<br>(ii) a signed document, workflow or email showing such persons have authorization and<br>(iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. |
| **Reference to prior version:**<br>*CIP 007-4 R5.1, CIP 004-4 R4* | | **Change Rationale:** *CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a “need to know” basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.* | |

**CIP-004-5 Table R6 – Access Management Program**

| Part | Applicability | Requirements | Measures |
|---|---|---|---|
| 6.2 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. | Evidence may include, but is not limited to:<br>(i) a system generated list of people with unescorted physical access through the Defined Physical Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access,<br>(ii) a signed document, workflow or email showing such persons have authorization and<br>(iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. |
| **Reference to prior version:**<br>*CIP-006-4 R1.5* | | **Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.* | |

**CIP-004-5 Table R6 – Access Management Program**

| Part | Applicability | Requirements | Measures |
|---|---|---|---|
| 6.3 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. | Evidence may include, but is not limited to:<br>(i) a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access,<br>(ii) a signed document, workflow or email showing such persons have authorization and<br>(iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. |
| **Reference to prior version:**<br>*CIP-003-4 R5.2* | | **Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.* | |

| CIP-004-5 Table R6 – Access Management Program | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 6.4 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access. | Evidence may include, but is not limited to:<br>• Dated documentation of the verification between the system generated list of individuals who have been authorized for access and a system generated list of personnel who have access<br>• Documentation of the dated verification between a list of individuals who have been authorized for access and a list of individuals provisioned for access. |
| **Reference to prior version:**<br>*CIP 004-4 R4.1* | | **Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.* | |

**CIP-004-5 Table R6 – Access Management Program**

| Part | Applicability | Requirements | Measures |
|---|---|---|---|
| 6.5 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. | Evidence may include, but is not limited to, documentation of the review including<br>(i) a dated listing of all accounts/account groups or roles within the system,<br>(ii) a summary description of privileges associated with each group or role,<br>(iii) accounts assigned to the group or role and (iv) 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. |
| **Reference to prior version:**<br>*CIP 007-4 R5.1.3* | | **Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.* | |

**CIP-004-5 Table R6 – Access Management Program**

| Part | Applicability | Requirements | Measures |
|---|---|---|---|
| 6.6 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions. | Evidence may include, but is not limited to documentation of the review including<br>(i) a dated listing of authorizations for BES Cyber System information,<br>(ii) any privileges associated with the authorizations, and<br>(iii) dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. |
| **Reference to prior version:**<br>*CIP-003-4 R5.1.2* | | **Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.* | |

**Rationale for R7:** The timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address the FERC Order directing immediate revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e. revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

**Summary of Changes:** Paragraphs 460 and 461 of FERC Order 706 state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

**R7.** Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]*

**M7.** Evidence must include each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| CIP-004-5 Table R7 – Access Revocation | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 7.1 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time[2] of the resignation or termination. | Evidence may include, but is not limited to<br>(i) workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action, and<br>(ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access. |
| **Reference to prior version:**<br>*CIP 004-4 R4.2* | | **Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.* | |

[2] Since a termination action is often recorded without consideration to the time of day, "at the time" does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action.

| **CIP-004-5 Table R7 – Access Revocation** | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 7.2 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | For reassignments or transfers, revoke the individual’s unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day. | Evidence may include, but is not limited to,<br>(i) workflow or sign-off form showing the review of logical and physical authorizations dated on the same calendar day as the transfer or reassignment and<br>(ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access where the review determined it was no longer needed. |
| **Reference to prior version:**<br>*CIP-004-4 R4.2* | | **Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.* | |

| CIP-004-5 Table R7 – Access Revocation | | | |
|---|---|---|---|
| **Part** | **Applicability** | **Requirements** | **Measures** |
| 7.3 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination. | Evidence may include, but is  not limited to, workflow or sign-off 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 calendar day of the termination action. |
| **Reference to prior version:**<br>*NEW* | | **Change Rationale:** *The FERC Order 706 Paragraph 386 directs modifications to the Standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.* | |

| CIP-004-5 Table R7 – Access Revocation | | | |
|---|---|---|---|
| Part | Applicability | Requirements | Measures |
| 7.4 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation. | Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revoking of access and dated within thirty calendar days of the termination. |
| **Reference to prior version:**<br>*NEW* | | **Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.* | |

**CIP-004-5 Table R7 – Access Revocation**

| Part | Applicability | Requirements | Measures |
|---|---|---|---|
| 7.5 | High Impact BES Cyber Systems<br>Medium Impact BES Cyber Systems.<br>Associated Physical Access Control Systems<br>Associated Electronic Access Control or Monitoring Systems<br>Associated Protected Cyber Assets | For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user.<br>In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances. | Evidence may include, but is not limited to:<br>• Workflow or sign-off form showing password reset within thirty calendar days of the termination<br>• Workflow or sign-off form showing password reset within thirty calendar days of the reassignments or transfers. |
| **Reference to prior version:**<br>*CIP-007 R5.2.3* | | **Change Rationale:**<br>*To provide clarification of expected actions in managing the passwords* | |

## C. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

#### 1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

#### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

#### 1.4. Additional Compliance Information

None

## Table of Compliance Elements

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| **R1** | **Operations Planning** | **Lower** | N/A | N/A | The Responsible Entity did not provide on-going security awareness reinforcement on at least a quarterly basis. (1.1) | The Responsible Entity did not document or implement a security awareness program. (R1) |
| **R2** | **Operations Planning** | **Lower** | N/A | N/A | The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include training for one or more of the roles as detailed in 2.2 through 2.10. | The Responsible Entity did not have the required role-based training. (R2) |
| **R3** | **Operations Planning.** | **Medium** | N/A | N/A | The Responsible Entity trained some but not all individuals authorized for electronic or unescorted physical access at least once every calendar year, but not to exceed 15 | The Responsible Entity trained some, but not all individuals authorized for electronic or unescorted physical access prior to their being granted such access, except in |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| | | | | | months between training. (3.2) | policy-identified CIP Exceptional Circumstances. (3.1)<br>OR<br>The Responsible Entity did not fully implement its cyber security training program. |
| **R4** | **Operations Planning** | **Medium** | N/A | The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1)(4.2) | The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5) | The Responsible Entity did not have a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access. (R4) |
| **R5** | **Same Day** | **Medium** | N/A | N/A | The Responsible Entity | The Responsible Entity |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| | Operations | | | | did perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances, but the personnel risk assessments are not updated at least once every seven years. (5.2) | did not perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances. (5.1)<br>OR<br>The Responsible Entity did not have a documented process for personnel risk assessments. |
| R6 | Operations Planning and Same Day Operations | Lower | The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work | The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work | The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work | The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| | | | functions. (6.1) (6.2)<br>OR<br>The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions. (6.3) | functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2)<br>OR<br>The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.3) | functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2)<br>OR<br>The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.3) | functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2)<br>OR<br>The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.3)<br>OR<br>The Responsible Entity did not perform a |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| | | | | | | quarterly verification of individuals with authorized access against one or more lists of individuals provisioned for unescorted physical or electronic access to BES Cyber Systems. (6.4)<br>OR<br>The Responsible Entity did not verify provisioned accounts/account groups or role categories and their specific, associated privileges according to the timeframe in CIP-004-5 6.5 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.5)<br>OR |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| | | | | | | The Responsible Entity did not verify the access privileges to BES Cyber System Information according to the timeframe in CIP-004-5 6.6 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.6)<br>OR<br>The Responsible Entity did not identify when CIP Exceptional Circumstances were invoked and/or revoked (6.7)<br>OR<br>The Responsible Entity did not have a documented process for access management. |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| **R7** | **Same Day Operations**<br>**and Operations Planning** | **Medium** | N/A | The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for one individuals who was terminated, resigned, reassigned, or transferred. (7.1 and 7.2) | The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred. (7.1 and 7.2) | The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2)<br>OR<br>The Responsible Entity did not have a documented process for access revocation. |

## D. Regional Variances

None.

## E. Interpretations

None.

## F. Associated Documents

None.

## Guidelines and Technical Basis

**Requirement R1:**

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

**Requirement R2:**

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the following required items appropriate to personnel roles and responsibilities from Table R4. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of “role appropriate” as it is used in this standard.

**Requirement R3:**

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

**Requirement R4:**

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-011-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their identity verified, then been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

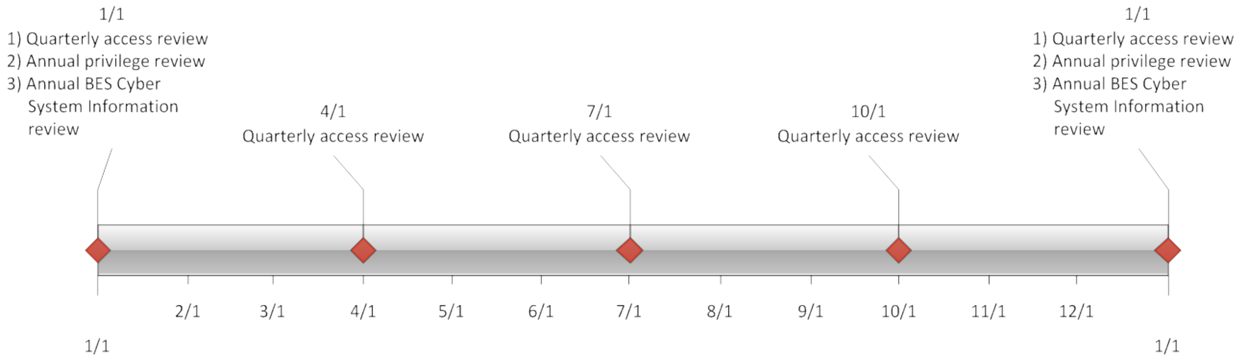
When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven year check could not be performed.  Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

**Requirement R6:**

Authorization for electronic and unescorted physical access and access to BES Cyber System information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual’s associated privileges are the minimum necessary to perform their work function (i.e. least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g. system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in R6 is included below.


1/1
1) Quarterly access review
2) Annual privilege review
3) Annual BES Cyber System Information review
4/1
Quarterly access review
7/1
Quarterly access review
10/1
Quarterly access review
1/1
1) Quarterly access review
2) Annual privilege review
3) Annual BES Cyber System Information review
2/1
3/1
4/1
5/1
6/1
7/1
8/1
9/1
10/1
11/1
12/1
1/1
1/1

Separation of duties should be considered when performing the reviews in R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

**Requirement R7:**

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

| Scenario | Possible Process |
|---|---|
| Immediate involuntary termination | Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process. |
| Scheduled involuntary termination | Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination. |
| Termination prior to notification | Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination. |
| Voluntary termination | Human resource personnel are notified of the termination and works with appropriate personnel to schedule the revocation of access at the time of termination. |
| Retirement where the last working day is several weeks prior to the termination date | Human resource personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day. |
| Death | No action is required. |

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in 7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents an Entity from performing all of the access revocation at the time termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.