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).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014

3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, 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. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted for final ballot. The draft includes modifications to meet FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014
~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

Effective Dates

1. **24 Months Minimum –** CIP-004-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

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. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	~~12/30/10~~1/24/11	~~Modified to add specific criteria for Critical Asset identification.~~ Approved by the NERC Board of Trustees.	~~Update~~
~~4~~5	~~1/24/~~11/26/12	~~Approved~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata

~~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 ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

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

2. **Number:** CIP-004-~~5.1~~6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. 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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional 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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   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 interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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 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. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional 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 ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional 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 interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~5.1~~6:

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. 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.

4.2.3.4. For Distribution Providers, 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-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-6.

6. Background:

Standard CIP-004 ~~5.1~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require 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~~ and 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*.~~

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 ~~requirement's~~ common subject matter of the requirements.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

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 ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table~~. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities~~.

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.

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 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 UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS 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-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 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 (EACMS)** – 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 (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

~~**Rationale for R1:** Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.~~

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

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 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 requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 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	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

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
		authorized unescorted physical access to BES Cyber Systems.	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).

~~Reference to prior version:~~ ~~*CIP-004-4, R1*~~	**~~Change~~ Rationale~~: *Changed to remove*~~ for Requirement R2:** To ensure that the Responsible Entity's training program for personnel who need ~~*to ensure or prove everyone with*~~ authorized electronic access and/or authorized unescorted physical access ~~*"received" ongoing reinforcement – to state that security awareness has been reinforced.*~~ ~~*Moved example mechanisms to guidance.*~~to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

~~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 covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.~~

~~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 implement~~, in a manner that identifies, assesses, and corrects deficiencies, a~~ 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-~~5.1~~6 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 requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.1*~~		~~**Change Rationale:** *Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. 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 No. 706, Paragraph 413. 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 No. 706, Paragraph 434.*~~	

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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.
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.1*~~		~~**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*~~	
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

~~Reference to prior version:~~	~~Change~~ Rationale~~: *Updated*~~ for Requirement R3:
~~*CIP004-4, R2.3*~~	To ensure that individuals who need authorized electronic or authorized unescorted physical access to ~~*replace "annually"*~~BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with ~~*"once every 15 calendar months."*~~ access must have had a personnel risk assessment completed within the last 7 years.

~~**Rationale for R3:** To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.~~

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

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment ~~programs~~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-~~5.1~~6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: 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-~~5.1~~6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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.
~~**Reference to prior version:**~~ ~~*CIP004-4, R3.1*~~		~~**Change Rationale:** *Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*~~	

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

~~**Reference to prior version:**~~ ~~*CIP004-4, R3.1*~~CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program	~~**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided 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.*~~

~~CIP-004-5.1 Table R3 – Personnel Risk Assessment Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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.
~~Reference to prior version:~~ ~~*NEW*~~		~~Change Rationale: *There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.*~~	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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.

~~Reference to prior version:~~ ~~*CIP-004-4, R3.3*~~	~~Change Rationale: *Separated into its own table item.*~~		
CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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.

~~Reference to prior version:~~

~~*CIP-004-3, R3, R3.3*~~

~~Change~~ Rationale~~: *Whether*~~ **for** ~~*initial access or maintaining access, establishes*~~**Requirement R4:**

To ensure that ~~*those*~~individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity 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 included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must ~~*have had PRA completed within 7 years.*~~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-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This ~~*covers both initial and renewal.*~~is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The ~~*implementation plan specifies that initial performance*~~focus of this requirement is ~~*7 years after the last personnel risk assessment*~~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 SDT intends that ~~*was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.*~~ 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 Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

~~Rationale for R4:~~ ~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity 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 included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.~~

~~Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System 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 Part 4.5 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 access 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 SDT intends that 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 Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.~~

~~Summary of Changes:~~ ~~The primary change was in 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.~~

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program. [Violation Risk Factor: ~~Lower~~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-~~5.1~~6 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-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Reference to prior version: *CIP-003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1*	**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. 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-004-5.16 Table R4 – Access Management Program

~~CIP-004-5.1 Table R4 – Access Management Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

~~**Reference to prior version:**~~ ~~*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, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*~~CIP-004-~~5~~.16 Table R4 – Access Management Program

~~CIP-004-5.1 Table R4 – Access Management Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar 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.

~~*Reference to prior version:*~~ ~~*CIP-007-4, R5.1.3*~~CIP-004-~~5.1~~6 Table R4 – Access Management Program	~~**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.*~~

~~CIP-004-5.1 Table R4 – Access Management Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

~~Reference to prior version:~~ *~~CIP-003-4, R5.1.2~~*	**~~Change Rationale:~~** *~~Moved requirement to ensure consistency among access reviews. Clarified precise meaning of 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 Requirement R5:** The timely revocation of electronic access to BES 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 directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., 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 physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System 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 (e.g., physical access control system, remote access system, directory services).

~~**Rationale for R5:** The timely revocation of electronic access to BES 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 directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., 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 physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System 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 (e.g., physical access control system, remote access system, directory services).~~

~~**Summary of Changes:** FERC Order No. 706, Paragraphs 460 and 461, 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."~~

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation*. *[Violation Risk Factor: ~~Lower~~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-~~5.1~~6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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.

~~Reference to prior version:~~ **CIP-004-**~~4, R4.2~~6 Table R5 – Access Revocation	**~~Change Rationale:~~** ~~*The FERC Order No. 706, Paragraphs 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.*~~

~~CIP-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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 calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

~~Reference to prior version:~~ **CIP-004-~~4, R4.2~~6 Table R5 – Access Revocation**	**~~Change Rationale:~~** *~~FERC Order No. 706, Paragraph 460 and 461, direct 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-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of 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: NEWCIP-004-5.16 Table R5 – Access Revocation	**Change Rationale:** *FERC Order No. 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-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar 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 BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Reference to prior version: NEWCIP-004-5.16 Table R5 – Access Revocation	**Change Rationale:** FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible 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-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar 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 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.
~~**Reference to prior version:**~~ ~~*CIP-007-4, R5.2.3*~~		~~**Change Rationale:**~~ ~~*To provide clarification of expected actions in managing the passwords.*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~(""~~ (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Violation Investigations

Self-Reporting

- ~~Complaint~~

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	~~and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized	~~and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	~~identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date~~, and did not identify, assess and correct the deficiencies~~. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals~~, and did not identify, assess, and~~	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals~~, and did not identify, assess, and~~	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	~~correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	~~correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date ~~and has identified deficiencies, and did not identify, assess, and correct the deficiencies~~. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)			
R4	**Operations Planning and Same Day Operations**	~~Lower~~Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter~~, and did not identify, assess and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located~~, and did not identify, assess, and correct the deficiencies~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.4)			were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that~~-~~ an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances~~, and did not~~			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~identify, assess, and correct the deficiencies~~. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce 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 and evidence, when dated, 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.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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 CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

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, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed 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, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last

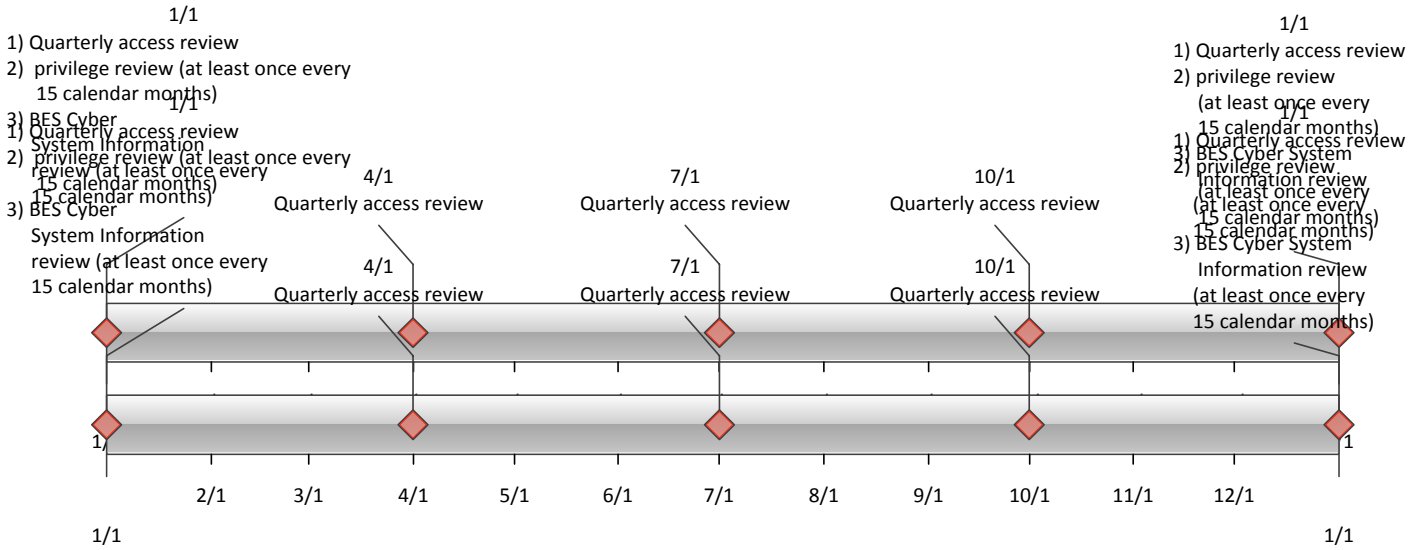
PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

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 where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. 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 privilege review at least once every 15 calendar months 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 Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this 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 Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

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 scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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 resources 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 resources personnel are notified of the termination and work 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 resources 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	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

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 Requirement R5.1 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 (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should 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.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.