Standard Development Timeline

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

Development Steps Completed

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

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. 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 ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-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 formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-004-5 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. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-004-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. 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	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

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

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

~~A.~~ Introduction

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

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

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the 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 ~~against compromise that could lead to misoperation or instability in the BES.~~.

4. **Applicability:**

   4.1. Functional Entities: ~~———~~ For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

   4.1.1. Balancing Authority

   ~~**4.1.2. Distribution Provider** that owns **Facilities described in 4.2.2**~~

   ~~**4.1.3. Generator Operator**~~

   ~~**4.1.4. Generator Owner**~~

   ~~**4.1.5. Interchange Coordinator**~~

   ~~**4.1.6. Load-Serving Entity that owns Facilities described in 4.2.1**~~

   ~~**4.1.7. Reliability Coordinator**~~

   ~~**4.1.8. Transmission Operator**~~

   ~~**4.1.9. Transmission Owner**~~

   ~~**4.2. Facilities:**~~

   ~~**4.2.1. Load-Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load-shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load-shedding under a common control system, without human operator initiation, of 300 MW or more.~~

   ~~**4.2.2**~~**4.1.2.** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

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

4.1.2.1.1. is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

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. ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~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 or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme 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.

~~4.2.3~~4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities: All BES Facilities.~~:

All BES Facilities.

~~4.2.4~~4.2.3. Exemptions: The following are exempt from Standard CIP-~~002~~004-5:

~~4.2.4.1~~4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~4.2.3.3. ~~In nuclear plants, the Systems~~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 identification and categorization processes.

5. Background:

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

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 ~~a~~the requirement's common subject matter.

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,** . . .

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

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

~~**Applicability Columns in Tables:**~~

~~Each table row~~ 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 ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies~~ to BES Cyber Systems and associated Cyber Assets~~. 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 ~~applicability~~"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 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity~~ or dial-up connectivity~~.
- ~~**Associated**~~ **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber

System ~~in the applicability column~~. Examples include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- ~~**Associated**~~ **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity ~~in the applicability column~~.

~~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.

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

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

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~A security~~Security awareness ~~program~~ that, at least once each calendar quarter, ~~conveys ongoing reinforcement of~~reinforces cyber security practices and associated physical security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	~~Evidence must include the documented security awareness program, and additional~~ An example of evidence ~~to demonstrate that this program was implemented. Evidence of implementation~~ may include, but is not limited to, documentation that the quarterly reinforcement has been provided. ~~Evidence~~ Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure or prove everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that ~~the program conveys~~security awareness ~~and measures that reinforcement "~~has been ~~provided."~~reinforced.* *Moved example mechanisms to guidance.*	

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
		~~*Changed to record delivery.*~~	

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 ~~have~~implement, in a ~~role-based~~manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to ~~attain and retain authorized electronic access~~individual roles, functions, or ~~authorized unescorted physical access to BES Cyber Systems that~~ responsibilities that collectively includes each of the applicable ~~items~~requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable ~~items~~requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*~~.~~ and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.1~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Identification of each role and training required for each role.~~	~~Acceptable evidence must include a list of roles and what training is needed for each role.~~
~~**Reference to prior version:** NEW~~		~~**Change Rationale:** *The first thing needed in a role-based training program is to understand what roles individuals have so that the Responsible Entity can plan what training modules it needs to provide.*~~	

~~2.2~~**Part**	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring~~**Applicable Systems**	~~Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems.~~**Requirements**	~~Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.~~**Measures**
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.1*~~	~~**Change Rationale:** *Removed to address 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.*~~		

CIP-004-5 Table R2 – Cyber Security Training Program				
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~	
2.~~3~~1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Training content on ~~the physical~~: 2.1.1. Cyber security policies; 2.1.2. Physical access controls ~~protecting the Responsible Entity's~~; 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	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials ~~on the proper use of physical access controls for BES Cyber Systems.~~.

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~Reference to prior version:~~ ~~*CIP004-4, R2.2.1 and R2.2.2*~~		~~Change Rationale:~~ ~~*Minor wording changes.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
Reference to prior version: *CIP004-4, R2.*2.~~4~~1	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.~~	**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.* ~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic access controls to protect BES Cyber Systems.~~

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the visitor control program.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the visitor control program.
Reference to prior version: *NEW*		**Change Rationale:** *No significant change from previous versions.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.6~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on handling of BES Cyber System Information and its storage.~~	~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the handling of BES Cyber System Information, including its storage.~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.3*~~		~~**Change Rationale:** *Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage media; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program				
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~	
2.~~7~~2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Training content on identification of a potential BES Cyber Security Incident and initial notifications in accordance with the entity's incident response plan~~ 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.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, training ~~material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the identification of a potential BES Cyber Security Incident~~records and ~~associated notifications~~documentation of when CIP Exceptional Circumstances were invoked.	
Reference to prior version: ~~*CIP-004-4, R2.2.4 (new; implied but not stated in CIP-004-4 or CIP-008-4)*~~*CIP004-4, R2.1*		**Change Rationale:** ~~*Core training on the identification and reporting*~~*Addition of* ~~*a Cyber Security Incident;*~~ *exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph* ~~*413; Related to*~~*431 is detailed in CIP-*~~*008*~~*003-5* ~~*& DHS Incident Reporting requirements for those with roles in incident reporting*~~*.*		

CIP-004-5 Table R2 – Cyber Security Training Program				
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~	
2.~~8~~3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS		~~Training content on recovery plans for BES Cyber Systems.~~Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, dated individual training ~~material such as power point presentations, instructor notes, student notes, handouts, or other training materials on recovery plans for BES Cyber Systems~~records.
Reference to prior version: *CIP004-4, R2.~~2.4~~3*			**~~Change Rationale:~~ Change Rationale:** *Updated to replace "annually" with "once every 15 calendar months."* ~~*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.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.9~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on response to BES Cyber Security Incidents.~~	~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the response to a BES Cyber Security Incident.~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.4*~~		~~**Change Rationale:** *Minor wording changes.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.10~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.~~	~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic interconnectivity and interoperability with other Cyber Assets.~~
~~**Reference to prior version:**~~ ~~*NEW*~~		~~**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*~~	

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

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

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

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

CIP-004-5 Table R3 – Cyber Security Training

Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access and authorized unescorted physical access to BES Cyber Systems, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring authorized electronic or authorized unescorted physical access, dated individual training records, the date authorized electronic or authorized unescorted physical access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
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.*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

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

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

~~**R4.** Each Responsible Entity shall have~~

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 to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively ~~includes~~include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

~~M4~~M3. Evidence must include the documented personnel risk assessment ~~program~~programs that collectively ~~includes~~include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program~~.~~* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~4~~3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~ EACMS; and 2. PACS	~~An initial personnel risk assessment ("PRA") that includes~~Process to confirm identity ~~verification~~.	~~Acceptable~~An example of evidence ~~must~~may include, but is not limited to, documentation of the ~~documented personnel risk assessment program with a requirement for an initial personnel risk assessment that includes~~Responsible Entity's process to confirm identity ~~verification~~.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identity ~~verification~~confirmation is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~4~~3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~ EACMS; and 2. PACS	~~Seven~~ Process to perform a seven year criminal history records check ~~including~~as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration~~,~~; and ~~covering at least all~~ 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~~:~~. ~~4.2.1. resided;~~ ~~4.2.2. been employed (if applicable); and~~ ~~4.2.3. attended school (if applicable).~~ If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	~~Acceptable~~An example of evidence ~~must~~may include, but is not limited to, documentation of the ~~documented personnel risk assessment program with a requirement for~~Responsible Entity's process to perform a seven~~-~~year criminal history ~~record~~records check ~~in accordance with this part.~~ ~~.~~

Reference to prior version: *CIP004-4, R3.1*	**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided~~, been employed, and/or attended school~~ for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*

CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~4~~3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~ EACMS; and 2. PACS	Process ~~or criteria used~~ to evaluate ~~personnel risk assessments to determine when to deny authorized~~criminal history records checks for authorizing access.	~~Acceptable~~An example of evidence ~~must~~may include, but is not limited to, documentation of the ~~documented personnel risk assessment program with the~~Responsible Entity's process ~~or criteria identified~~to evaluate criminal history records checks.
Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate ~~personnel risk assessments~~criminal history records checks for authorizing access.*	

~~4~~3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~ EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted ~~pursuant~~according to ~~CIP-004-5 R4,~~ Parts ~~4~~3.1 through ~~4~~3.3.	~~Acceptable~~An example of evidence ~~must~~may include, but is not limited to, documentation of the ~~documented personnel risk assessment program with the~~Responsible Entity's criteria or process ~~identified~~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 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 that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.*	

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

~~**R5.**~~

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 ~~one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems~~, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

~~collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*~~

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

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

CIP-004-5 Table R5 — Personnel Risk Assessment			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update each personnel risk assessment at least once every seven calendar years after the initial or previous personnel risk assessment such that the current PRA is no older than seven years.	Evidence may include, but is not limited to, current and previous personnel risk assessment records.
Reference to prior version: *CIP-004-4, R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

Rationale for R6: To ensure that individuals with access to BES Cyber Systems 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 all 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 6.5 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 R6 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.

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

~~**M6**~~**M4.** Evidence must include the documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R6~~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.

~~**Reference to prior version:**~~ ~~*CIP-003-4, R5.1; CIP-007-4, 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-004-5 Table R6 – Access Management Program**~~			
~~**Part**~~	~~**Applicability**~~	~~**Requirements**~~	~~**Measures**~~
~~6.2~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.~~	~~Evidence may include, but is not limited to, a signed document, automated workflow approval, or email showing persons with electronic access have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.~~

CIP-004-5 Table ~~R6~~R4 – Access Management Program			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**

CIP-004-5 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.*

~~6.3~~4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	~~The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.~~ Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	~~Evidence~~Examples of evidence may include, but ~~is~~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 ~~people with unescorted physical access, a signed document, automated workflow approval, or email showing persons with unescorted physical~~personnel who have access ~~have~~ (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~~, and similar~~ forms) and a list of individuals provisioned for access (i.e., provisioning forms or ~~the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.~~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 Table R6 – Access Management Program~~			
~~Part~~	~~Applicability~~	~~Requirements~~	~~Measures~~

6.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	The individual(s) designated in Part 6.1 shall authorize access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	A signed document, automated workflow approval or email showing persons with access to BES Cyber System Information have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4, R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Verify at least once each calendar quarter that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.	Evidence may include, but is 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 • Documentation of the dated 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).

CIP-004-5 Table ~~R5~~R4 – Access Management Program			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~6.6~~4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	For electronic access, verify at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between verifications,~~ 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 ~~for performing assigned work functions~~.	~~Evidence~~An example of evidence may include, but is not limited to, documentation of the review ~~including~~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*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary ~~for performing assigned work functions.~~.*	

CIP-004-5 Table ~~R5~~R4 – Access Management Program			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~6.7~~4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	Verify at least once ~~per calendar year, but not to exceed~~every 15 calendar months ~~between verifications,~~ that access to the ~~physical and electronic~~designated storage locations ~~where~~for BES Cyber System Information ~~is stored by the Responsible Entity,~~ whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	~~Evidence~~An example of evidence may include, but is not limited to, the ~~following~~ 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 R5~~7~~: 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 (~~i.e.~~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 all 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).

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."

~~**R7**~~

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R7~~R5 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning].*

~~M7~~M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R7~~R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~For all termination actions, initiate the~~A process to ~~revoke the~~initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon ~~the effective date and time of the~~a termination action, and complete the ~~revocation~~removals within 24 hours ~~after the effective date and time~~ of the termination action~~.~~ (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	~~Evidence~~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.
~~7~~~~Reference~~Reference to prior version: *CIP 004-4, R4.2*	**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 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic ~~and~~access to individual accounts and authorized unescorted physical access that the Responsible Entity determines ~~is~~are not necessary by the end of the next calendar day following the ~~reassignment or transfer~~date that the Responsible Entity determines that the individual no longer requires retention of that access.	~~Evidence~~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*		**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 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the ~~physical and electronic~~ designated storage locations ~~where~~for BES Cyber System Information ~~is stored by the Responsible Entity~~, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date and time of the termination action.	~~Evidence~~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: *NEW*		**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 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.4	High Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ • EACMS	For termination actions, revoke the individual's non-shared user accounts ~~on BES Cyber Assets~~ (unless already revoked ~~in accordance with Requirements R7~~according to Parts 5.1 or ~~R7~~5.3) within 30 calendar days of the effective date of the termination action.	~~Evidence~~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: *NEW*		**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 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.5	High Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ • EACMS	For termination actions~~, reassignments, or transfers~~, change passwords for shared account(s) known to the user within 30 calendar days of the termination action~~, reassignment, or transfer of the user.~~. 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.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; ~~or~~ • 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 the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~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 ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years ~~or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~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
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so beyond 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not document a security awareness program. (R1)
R2	Operations Planning	Lower	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 1 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 2 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 4 or more of the training content as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	Operations Planning.	Medium	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			train 1 individual prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 1 individual authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 2 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 2 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 3 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 3 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 4 or more individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 4 or more individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2) OR The Responsible Entity did not implement at all its cyber security training program. (R3)
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in	The Responsible Entity has a personnel risk assessment program, as stated in	The Responsible Entity did not have a personnel risk assessment program,

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	Same Day Operations	Medium	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 1 individual prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 2 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR The Responsible Entity did not update	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 3 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR	The Responsible Entity did not have a documented process for personnel risk assessments. (R5) OR Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 4 or more individuals

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not update personnel risk assessments every seven years for 1 individual within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	personnel risk assessments every seven years for 2 individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	The Responsible Entity did not update personnel risk assessments every seven years for 3 or more individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1)
R6	Operations Planning and Same Day Operations	Lower	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not have a documented process for access management. (R6) OR The Responsible Entity did not designate one or more individual(s) to authorize electronic access, unescorted physical access, or access to the physical and electronic

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			determined was necessary for performing assigned work functions. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 17 calendar months but not within 15 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that that the Responsible	determined was necessary for performing assigned work functions and one user was granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within the calendar quarter that individuals provisioned for unescorted physical access and electronic access had associated authorization records. (6.5) OR The Responsible Entity did verify within 19 calendar months but not within 17 calendar months that: (6.6)	determined was necessary for performing assigned work functions and two users were granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 21 calendar months but not within 19 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories are correct, or • their specific, associated privileges were	locations where BES Cyber System Information is stored by the Responsible Entity. (6.1) OR The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary for performing assigned work functions and three or more users were granted access without authorization

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	(6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System	correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for	by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within 24 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were the those that that the Responsible Entity determined necessary for

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	performing assigned work functions.	performing assigned work functions, or • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.
R7	Same Day Operations and Operations Planning	Medium	Revocation of access to BES Cyber Information was not accomplished for 1 or more individuals	The Responsible Entity did not revoke unneeded unescorted physical or electronic access within the	The Responsible Entity did not revoke unneeded unescorted physical or electronic access according to	The Responsible Entity did not have a documented process for initiating the unescorted physical or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within the specified time frame (7.3); OR User accounts on BES Cyber Assets were not revoked for one or more individuals within the specified time frame (7.4); OR User passwords on BES Cyber Asset shared accounts were not changed for one or more individuals within the specified time frame; (7.5) OR Following the determination and documentation of extenuating operating circumstances, passwords for shared accounts were not changed for one or	specified times in CIP-004-5 R7 for one individual who was terminated, resigned, was reassigned, or transferred. (7.1 and 7.2)	the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred.(7.1 and 7.2)	electronic access revocation process; OR The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more individuals within 10 days following the end of the extenuating operating circumstances. (7.5)			

~~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 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 ~~reference sound~~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.).

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

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the 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.

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

~~Requirement R3:~~

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 does not require reconfirmation during the tenure of employment.

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

~~Requirement R4 and R5:~~

~~Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-004-1 Table R4 – Personnel Risk Assessment, 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, to ensure that personnel who have such access have had their identity verified, then been assessed for risk,~~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.

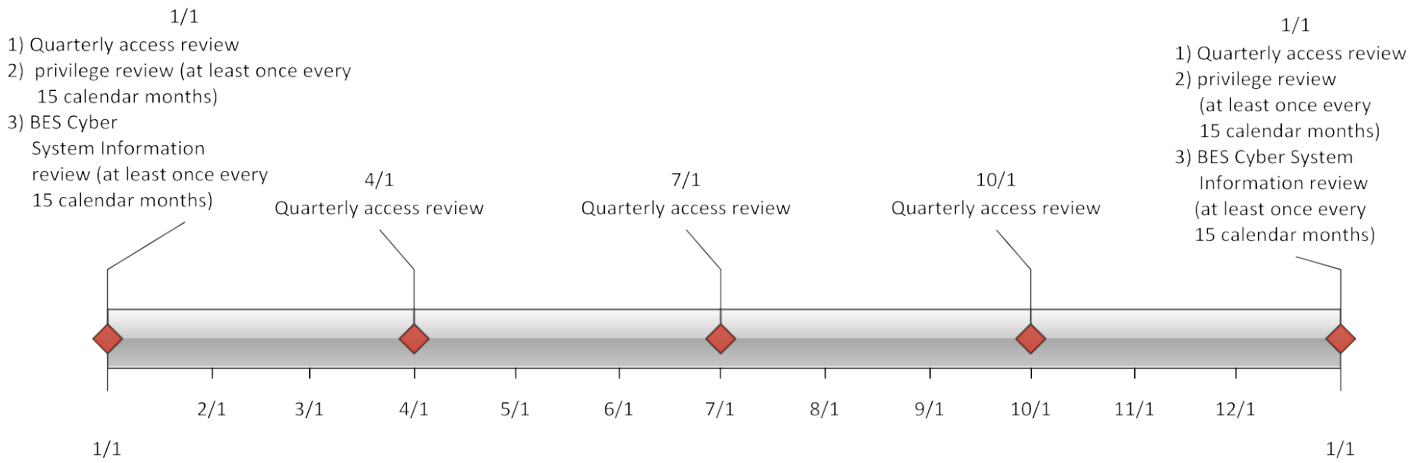
When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, ~~or~~ 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 ~~R6~~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 ~~and annual~~ 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 ~~annual~~ 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 ~~R6~~R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement ~~R6~~R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or ~~annual~~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 ~~R6~~R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement ~~R7~~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 ~~examples~~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.
~~Termination prior to notification~~	~~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 ~~R7~~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, ~~the requirement states~~ a review of access privileges ~~must~~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.