Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29 2023

Anticipated Actions	Date
Final Ballot	April 3 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

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

2. **Number:** CIP-004-8

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

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

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

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. 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 RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

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

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. 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.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) 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 BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part	months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part		
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are 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.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Examples of evidence may include, but are 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.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • 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.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

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

   The applicable 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:

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

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity did not revoke individual's user accounts upon termination action within 30 calendar days of the date of	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-004-8 Technical Rationale

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	TBD	Virtualization Modifications	