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

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2 – 11, 2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

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

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

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

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this 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-X:

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

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

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-X.

6. **Background:** Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

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

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

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-X 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-X Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other	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-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
		Cyber Assets, including Transient Cyber Assets, and with Removable Media.	
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-X 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-X Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	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	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-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	their associated: 1. EACMS; and 2. PACS		
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.

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-X 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-X 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-X Table R2 – Cyber Security Training 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; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS		Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 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-X 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-X Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and Logs or other demonstration showing such persons no longer have access.
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact BES Cyber Systems and their	For termination actions, revoke the	An example of evidence may include,

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	associated: • EACMS	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.	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.
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

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-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X 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-X 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-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	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.	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-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) 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.

2. Table of Compliance Elements

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and

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

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within	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. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	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. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has not implemented any documented program(s) for access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	and Operations Planning		user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	the next calendar day following the predetermined date. (5.2)	the next calendar day following the predetermined date. (5.2)	access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

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.	

Version	Date	Action	Change Tracking
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 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	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.