

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 initial draft of 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–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-7
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, and security awareness 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-004-7:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation 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-002-5.1 identification and categorization processes.

4.3. “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. This concept was adapted 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.

5. Effective Dates: See “Project 2016-02 Virtualization 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-004-7 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-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BCS and their associated SCI Medium Impact BCS and their associated SCI	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 BCS or SCI.	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: <ul style="list-style-type: none"> • 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-004-7 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-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. Electronic Access Control or Monitoring System (EACMS); and 2. Physical Access Control Systems (PACS) <p>Medium Impact BCS, with External Routable Connectivity (ERC) or Interactive Remote Access (IRA), and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI, with ERC or IRA, hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>Training content on:</p> <ol style="list-style-type: none"> 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 and SCI; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS and SCI’s electronic interconnectivity and interoperability with other Cyber Assets and VCA, including Transient Cyber Assets, and with Removable Media. 	<p>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.</p>

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>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, VCA or SCI, except during CIP Exceptional Circumstances.</p>	<p>Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.</p>

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.3	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>Require completion of the training specified in Part 2.1 at least once every 15 calendar months.</p>	<p>Examples of evidence may include, but are not limited to, dated individual training records.</p>

- 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 BCS or their associated SCI that collectively include each of the applicable requirement parts in *CIP-004-7 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-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact BCS and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: <ul style="list-style-type: none"> • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: <ul style="list-style-type: none"> • EACMS; or • 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.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven-years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. <p>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.</p>	<p>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.</p>

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>Criteria or process to evaluate criminal history records checks for authorizing access.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to evaluate criminal history records checks.</p>

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.4	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>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.</p>	<p>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.</p>

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>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 to 3.4 within the last seven years.</p>	<p>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.</p>

- 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-004-7 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-004-7 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-004-7 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BCS and their associated:</p> <ul style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ul style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ul style="list-style-type: none"> 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BCSI. 	<p>An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BCSI.</p>

CIP-004-7 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>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.</p>	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 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.

CIP-004-7 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.4	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>Verify at least once every 15 calendar months that access to the designated storage locations for BCSI, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.</p>	<p>An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 1. A dated listing of authorizations for BCSI; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

- 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-004-7 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-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated EACMS or PACS. SCI with ERC or IRA hosting Medium Impact BCS or their associated EACMS or PACS.</p>	<p>A process to initiate removal of an individual’s ability for unescorted physical access and 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).</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 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.

CIP-004-7 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>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.</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 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-004-7 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BCS with ERC or IRA and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>SCI hosting High Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS <p>SCI with ERC or IRA hosting Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • EACMS; or • PACS 	<p>For termination actions, revoke the individual’s access to the designated storage locations for BCSI, whether physical or electronic (unless already revoked according to Requirement R5 Part 5.1), by the end of the next calendar day following the effective date of the termination action.</p>	<p>An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BCSI associated with the terminations and dated within the next calendar day of the termination action.</p>

CIP-004-7 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.4	<p>High Impact BCS and their associated:</p> <ul style="list-style-type: none"> EACMS <p>SCI hosting High Impact BCS or their associated EACMS.</p>	<p>For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.</p>	<p>An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any applicable systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.</p>
5.5	<p>High Impact BCS and their associated:</p> <ul style="list-style-type: none"> EACMS <p>SCI hosting High Impact BCS or their associated EACMS.</p>	<p>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.</p> <p>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.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> 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.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and 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-004-7)			
	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. (Requirement R1 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. (Requirement R1 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. (Requirement R1 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. (Requirement R1 Part 1.1)
R2	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2 Part R2) 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. (Requirement R2 Part 2.1)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>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. (Requirement R2 Part 2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15</p>	<p>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. (Requirement R2 Part 2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)</p>	<p>exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)</p>	<p>OR</p> <p>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. (Requirement R2 Part 2.2)</p> <p>OR</p> <p>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. (Requirement R2 Part 2.3)</p>

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar months of the previous training completion date. (Requirement R2 Part 2.3)			
R3	<p>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. (Requirement R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs)</p>	<p>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. (Requirement R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access</p>	<p>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. (Requirement R3)</p> <p>OR</p> <p>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.</p>	<p>The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3)</p> <p>OR</p> <p>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. (Requirement R3)</p>

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (Requirement R3 Part 3.1 & Part 3.4)</p> <p>OR</p> <p>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</p>	<p>but did not confirm identity for two individuals. (Requirement R3 Part 3.1 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (Requirement R3 Part 3.2 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized</p>	<p>(Requirement R3 Part 3.1 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (Requirement R3 Part 3.2 & Part 3.4)</p> <p>OR</p> <p>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</p>	<p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (Requirement R3 Part 3.1 & Part 3.4)</p> <p>OR</p> <p>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. (Requirement R3 Part 3.2 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized</p>

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>one individual. (Requirement R3 Part 3.2 & Part 3.4)</p> <p>OR</p> <p>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. (Requirement R3 Part 3.3 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel</p>	<p>unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (Requirement R3 Part 3.3 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)</p>	<p>three individuals. (Requirement R3 Part 3.3 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)</p>	<p>electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (Requirement R3 Part 3.3 & Part 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)</p>

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 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 calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2)	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. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to	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. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories,	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BCSI is located. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>OR</p> <p>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 5% or less of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the</p>	<p>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 5% but less than (or equal to) 10% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BCSI storage locations, privileges were incorrect or</p>	<p>and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)</p>	<p>OR</p> <p>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. (Requirement R4 Part 4.2)</p> <p>OR</p> <p>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 applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and</p>

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	unnecessary. Requirement R4 Part (4.4)		necessary within 15 calendar months of the previous verification but for more than 15% of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)
R5	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BCSI, but for one individual, did not do so by the end of the next calendar day following the effective date and time of the	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (Requirement R5 Part 5.1) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (Requirement R5 Part 5.1) OR	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BCSI storage locations. (Requirement R5 Part R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>termination action. (Requirement R5 Part 5.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (Requirement R5 Part 5.4)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts</p>	<p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BCSI but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the</p>	<p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for BCSI but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3)</p>	<p>did not initiate those removals for three or more individuals. (Requirement R5 Part 5.1)</p> <p>OR</p> <p>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 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. (Requirement R5 Part 5.2)</p>

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>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. (Requirement R5 Part 5.5)</p> <p>OR</p> <p>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</p>	<p>termination action. (Requirement R5 Part 5.3)</p>		

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Requirement R5 Part 5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

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	<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3	12/16/09	<p>Updated Version Number from -2 to -3</p> <p>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.</p>	
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

Version	Date	Action	Change Tracking
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 BCS.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	