The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

# 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 by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
4. **Applicability:**

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

**4.1.1.** **Balancing Authority**

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

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

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

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

**4.1.2.2.** 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 requirements in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirementswhere a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.

**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 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 BES Cyber Systems' Logical Isolation Zones.

**4.2.3.3.** Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

**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 BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

**5. Effective Dates:** See Implementation Plan for CIP-004-7.

## 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*.

**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 BES Cyber Systems<br><br>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:<br>• direct communications (for example, e-mails, memos, computer-based training); or<br>• indirect communications (for example, posters, intranet, or brochures); or<br>• 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*.

**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** | High Impact BES Cyber Systems and their associated:<br>1. EACS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS; and<br>2. PACS | Training content on:<br>2.1.1. Cyber security policies;<br>2.1.2. Physical access controls;<br>2.1.3. Electronic access controls;<br>2.1.4. The visitor control program;<br>2.1.5. Handling of BES Cyber System Information and its storage;<br>2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;<br>2.1.7. Recovery plans for BES Cyber Systems;<br>2.1.8. Response to Cyber Security Incidents; and<br>2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media. | Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials. |

| CIP-004-7 Table R2 – Cyber Security Training Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| **2.2** | High Impact BES Cyber Systems and their associated:<br>1. EACS; and<br>2. PACS<br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS; and<br>2. PACS | Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access, 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:<br>1. EACS; and<br>2. PACS<br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS; and<br>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-004-7 Table R3 – Personnel Risk Assessment Program*.

**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 BES Cyber Systems and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS | 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** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS | Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:<br>3.2.1. current residence, regardless of duration; and<br>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.<br><br>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check. |

| CIP-004-7 Table R3 – Personnel Risk Assessment Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| **3.3** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS<br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS | 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:<br>1. EACS;<br>2. PACS; and<br>3. PCS<br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS | 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-004-7 Table R3 – Personnel Risk Assessment Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| **3.5** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS<br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. PACS; and<br>3. PCS | 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. | 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-004-7 Table R4 – Access Management Program.*

**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** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS | Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:<br>4.1.1. Electronic access;<br>4.1.2. Unescorted physical access into a Physical Security Perimeter; and<br>4.1.3. Access to designated storage locations (including EAMS and PAMS whether physical or electronic, for BES Cyber System Information. | An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information. |

| CIP-004-7 Table R4 – Access Management Program | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| **4.2** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS | 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:<br>• 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<br>• 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** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS; and<br>4. PAMS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS; and<br>4. PAMS | 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:<br>1. A dated listing of all accounts/account groups or roles within the system;<br>2. A summary description of privileges associated with each group or role;<br>3. Accounts assigned to the group or role; and<br>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** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. EAMS; and<br>3. PACS; and<br>4. PAMS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. EAMS; and<br>3. PACS; and<br>4. PAMS | Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, including EAMS and PAMS are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions. | An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:<br>1. A dated listing of authorizations for BES Cyber System information;<br>2. Any privileges associated with the authorizations; and<br>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*.

**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** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS | 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:<br>1. Dated workflow or sign-off form verifying access removal associated with the termination action; and<br>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** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS<br><br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACMS;<br>2. EAMS;<br>3. PACS;<br>4. PAMS; and<br>5. PCS | 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:<br>1. Dated workflow or sign-off form showing a review of logical and physical access; and<br>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** | High Impact BES Cyber Systems and their associated:<br>1. EACS;<br>2. EAMS;<br>3. PACS; and<br>4. PAMS<br>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:<br>1. EACS;<br>2. EAMS; and<br>3. PACS; and<br>4. PAMS | For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), including EAMS and PAMS by the end of the next calendar day following the effective date of the termination action. | An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action. |
| **5.4** | High Impact BES Cyber Systems and their associated EACS. | For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action. | An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions. |

| CIP-004-7 Table R5 – Access Revocation | | | |
|---|---|---|---|
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| **5.5** | High Impact BES Cyber Systems and their associated EACS. | 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.<br><br>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:<br>• Workflow or sign-off form showing password reset within 30 calendar days of the termination;<br>• Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or<br>• 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 Assessment Processes:**

   - Compliance Audits
   - Self-Certifications
   - Spot Checking
   - Compliance Violation Investigations
   - Self-Reporting
   - Complaints

   **1.4. Additional Compliance Information:**
   None.

## 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.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | 12/16/09 | Updated Version Number from -2 to -3<br>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 | |