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 — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the requirements in this standard, 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 explicitly specified.

   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 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 requirements in this standard where 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-007-7:

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 (LIZ).

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-007-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by uncontrolled logical and physical connectivity that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – Connectivity*.

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – Connectivity* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– Connectivity			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Use one or a combination of the following methods (per system capability) excluding serial port connectivity such as RS-232 and RS-485: • Configure each system to provide only essential logical connectivity; • Detect and alert on malicious communication within systems; • Baseline system logical connectivity, and alert on deviation from baseline; or • Other method(s) to mitigate the risk posed by uncontrolled logical connectivity. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled logical ports. • Listings of logical listening ports on the applicable systems, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others. • Documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, privileged introspection, etc.) are implemented within systems. • Any necessary combination of configuration files of system connectivity, storage connectivity, or network connectivity.

CIP-007-7 Table R1– Connectivity			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCS; and 2. Nonprogrammable communication components located inside both a PSP and a LIZ. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCS; and 2. Nonprogrammable communication components located inside both a PSP and a LIZ.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unmanaged software that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Software Management*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Software Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Software Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Use one or a combination of the following methods (per system capability) to allow only essential software execution, as determined by the Responsible Entity: • Configure each system with intentionally installed essential software and executable scripts; • Baseline currently installed software and executable scripts and alert on any newly installed software or executable scripts; • Implement application whitelisting; • Use read-only bootable media; or • Other methods to mitigate the risk posed by unmanaged software. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to: • Documentation of essential software and executable scripts; • Application whitelisting rule sets; • Documentation of read-only bootable media configuration; or • Documentation of other methods.

R3. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by malicious code that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*.

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Deploy method(s) to deter, detect, or prevent malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Mitigate the threat of detected malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to monitor security events to mitigate the risk posed by detectable security incidents that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*.

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Log events (per system capability) for identification and subsequent investigations of Cyber Security Incidents that include each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types that the BES Cyber System can detect and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Generate alerts for security events that the Responsible Entity determines need an alert, that include, as a minimum, each of the following types of events (per system capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to, paper or system-generated lists of security events that the Responsible Entity determined need alerts, including paper or system generated lists showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACS; 2. PACS; and 3. PCS	Retain applicable event logs identified in Part 4.1 per system capability for at least the last 90 consecutive calendar days.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unauthorized electronic access that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*.

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Have a method(s) to enforce authentication of interactive user access, per system capability. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location or by system type(s). NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.
5.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are put in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the system; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the system.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

		NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Per system capability, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACS; 2. PACS; and 3. PCS	Per system capability, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

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. 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-007-5.	
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	2/15/15	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-007-6. Docket No. RM15-14-000	