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 ~~second~~ third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29–October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

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 (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

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-007-7:

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

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

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

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

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above.~~in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. ~~Enable only network accessible Internet Protocol (IP) ports (or services if unable to determine ports) determined to be needed by the Responsible Entity, including port ranges where needed to handle dynamic ports, per system capability. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible ~~IP~~ logical ports and network accessible logical services~~or services, individually or by group~~. • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls~~, policy,~~ or other device level mechanisms that disables or prevents unneeded network accessible logical services. ~~only allow needed IP ports or services and deny all others.~~

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~l~~impact BCS and their associated: 1. PCA; and 2. Non-programmable communications components located inside both a PSP and ESP~~.~~ Medium ~~l~~impact BCS at Control Centers and their associated: 1. PCA; and 2. Non-programmable communications components located inside both a PSP and ESP~~.~~ SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	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.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI ~~identified independently~~ supporting: • High ~~I~~impact BCS and their associated: 1. EACMS 2. PACS; and 3. PCA • Medium ~~I~~impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. ~~Prevent the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems.~~	Examples of evidence may include, but ~~is~~are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared ~~with non-CIP Systems~~.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

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 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above.~~in this Part	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable ~~S~~Systems that are updateable and for which a patching source exists.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System C~~component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System in this Part~~above~~	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

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 Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~l~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Deploy method(s) to deter, detect, or prevent malicious code.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Mitigate the threat of detected malicious code.	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.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI- ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	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 e~~Examples of evidence may include, but are~~is~~ not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

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-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an applicable system ~~above~~in this Part	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, 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; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High ~~i~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~i~~impact BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, at a minimum, each of the following types of events~~,~~ (per Cyber Asset or BCS ~~system~~ capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High ~~i~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~i~~impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	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 calendar days or greater.
4.4	High ~~i~~impact BCS and their associated: 1. EACMS; and 2. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Review a summarization or sampling of logged security 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, ~~any~~ 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) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

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 ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
5.2	High ~~I~~impact BCS and their associated:	Identify and inventory all known enabled default or other generic account types,	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, a

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	either by system, by groups of systems, by location, or by system type(s).	listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI- ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Identify individuals who have authorized access to shared accounts.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	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 in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique.
5.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	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 Applicable 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 Applicable 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.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	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, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account lockout parameters; or Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

	~~above~~in this Part		

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-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that include the applicable items in CIP-007-7 Table R1. (Requirement R1) ~~N/A~~	The Responsible Entity ~~has implemented and documented processes for system hardening but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (~~Requirement R1~~ Part 1.2) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for system hardening, but has not prevented the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems. (Requirement R1 Part 1.4)~~	The Responsible Entity ~~has implemented and documented processes for determining necessary system hardening, but~~ had one or more unneeded network accessible services enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. ~~implemented and documented processes for determining necessary system hardening, but had one or more unneeded services enabled.~~ (Requirement R1 Part 1.3)	The Responsible Entity ~~did not~~neither implemented nor document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for ~~a~~Applicable ~~s~~Systems. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the~~	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for installing cyber security patches for Applicable Systems. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (~~Requirement R2~~ Part 2.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable ~~systems~~Cyber Assets. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an~~

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	~~vulnerabilities exposed by applicable security patches,~~ did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (~~Requirement R2~~ Part 2.3)	The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (~~Requirement R2~~ Part 2.3)	~~applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (~~Requirement R2~~ Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as created or revised within the timeframe specified in the plan. (~~Requirement R2~~ Part 2.4)
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention~~	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		used, the Responsible Entity did not address testing the signatures or patterns. (~~Requirement R3~~ Part 3.3)	~~but~~ did not mitigate the threat of detected malicious code. (~~Requirement R3~~ Part 3.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity~~ did not update malicious code protections. (~~Requirement R3~~ Part 3.3).	included the applicable items in CIP-007-7 Table R3. (Requirement R3). OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (~~Requirement R3~~ Part 3.1)
R4	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar~~	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but~~ missed ~~an~~ one 15 calendar day interval and completed the review within 30	The Responsible Entity ~~has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R4. (Requirement R4) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~days but~~ missed ~~an~~one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (~~Requirement R4~~ Part 4.4)	calendar days of the prior review. (~~Requirement R4~~ Part 4.4)	for all of the required types of events described in 4.2.1 through 4.2.2. (~~Requirement R4~~ Part 4.2) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log applicable events identified in 4.1 (except during CIP Exceptional Circumstances) but~~ did not retain applicable event logs for at least the last 90 consecutive days. (~~Requirement R4~~ Part 4.3) OR The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling~~	The Responsible Entity ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but~~ did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (~~Requirement R4~~ Part 4.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (~~Requirement R4~~ Part 4.4)	
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (~~Requirement R5~~ Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (~~Requirement R5~~ Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of ~~-~~all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (~~Requirement R5~~ Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals with authorized	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (~~Requirement R5~~ Part 5.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to shared accounts. (~~Requirement R5~~ Part 5.3) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (~~Requirement R5~~ Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in	OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (~~Requirement R5~~ Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (~~Requirement R5~~ Part 5.4) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			5.5.1 and 5.5.2. (~~Requirement R5~~ Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (~~Requirement R5~~ Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity~~ did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (~~Requirement R5~~ Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, did not~~ neither limit the number of unsuccessful authentication attempts nor generate alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See "Project 2016-02 ~~Virtualization~~ Modifications to CIP Standards Implementation Plan".
- See Technical Rationale for CIP-007-7

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to

Version	Date	Action	Change Tracking
			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	
7	TBD	Virtualization modifications	