Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

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

A. Introduction

1. **Title:**   Cyber Security — System Security Management

2. **Number:**   CIP-007-76

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 ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ 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**~~**4.1.4**   ~~Interchange Coordinator or Interchange Authority~~

   ~~**4.1.6**~~**4.1.5**   **Reliability Coordinator**

4.1.74.1.6 **Transmission Operator**

4.1.84.1.7 **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 ~~SPS or~~ RAS where the ~~SPS or~~ 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-~~6~~7:

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

4.2.3.2 Cyber ~~Assets~~ systems associated with ~~communication networks and data~~ communication links ~~between discrete~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI). ~~Electronic Security Perimeters.~~

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.2~~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.

~~4.2.3.3~~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~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3.   **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5.   **Effective Dates:**

See "Project 2016-02 Virtualization Implementation Plan." ~~for CIP-007-76).~~

~~6.   Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

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

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

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

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training~~

program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

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

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

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

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

"Applicable Systems" Columns in Tables:

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

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems at Control Centers – Only applies to medium impact BES Cyber Systems located at a Control Center.

Medium Impact BES Cyber Systems with External Routable Connectivity – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

Electronic Access Control or Monitoring Systems (EACMS) – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Protected Cyber Assets (PCA) – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

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-007-6 7 Table R1 –* System Hardening*Ports and Services*. *[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-007-6 7 Table R1 –* System Hardening*Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R1– Ports and ServicesSystem Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems BCS and their associated: 1. EACMS 2. PACS; and 3. PCA Medium Impact BES Cyber SystemsBCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, Eenable only logical network accessible ports services that have been determined to be needed by the Responsible Entity, (or logical network accessible ports if unable to determine service, including port ranges or services where needed to handle dynamic ports), per system capability. If a device system has no provision for disabling or restricting network accessible services (or logical ports) on the device then those ports services (or logical ports), that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports, on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports, on the Cyber Assets, 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, policy, or other device level mechanisms that only allow needed ports and deny all others.

| 1.2 | High Impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA~~.; and~~

1. ~~Nonprogrammable communication components located inside both a PSP and an ESP.~~
Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated ~~:~~PCA ~~; and~~

1. ~~Nonprogrammable communication components located inside both a PSP and an ESP.~~
SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA

Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA

Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers | 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. |
| | SCI hosting High or Medium Impact BCS or their associated: | Enable only services that have been determined to be needed by the | Examples of evidence may include, but are not limited to: |

CIP-007-76 Table R1 – ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	• PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Responsible Entity, per system capability.	• Documentation of implemented hardening guidelines • Configuration management reporting that demonstrates the need for all enabled services.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-76 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-007-76 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	A patch management process for tracking, evaluating, and installing cyber security patches~~. for applicable Cyber Assets.~~ 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 systems ~~for applicable Cyber Assets~~ that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis. ~~.

CIP-007-76 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA~~; and~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA~~; and~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but 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-007-76 Table R2 – Security Patch Management		
Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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; ~~or~~ • 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 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 patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System 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 security patch and a timeframe for the completion of these mitigations.

CIP-007-76 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-76 Table R3 – Malicious Code ProtectionPrevention. [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-007-76 Table R3 – Malicious Code ProtectionPrevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R3 – Malicious Code ProtectionPrevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Deploy method(s) to deter, detect, or prevent malicious code.	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, white-listing, privileged introspection, etc.).

CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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-007-76 Table R3 – Malicious Code ProtectionPrevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber SystemsBCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber SystemsBCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-76 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-007-76 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-76 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Log security events, per system capability, ~~at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Aasset level (per Cyber Aasset capability)~~ for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, at~~s~~ 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; 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 ~~BES Cyber System~~ BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

| 4.2 | High Impact ~~BES Cyber Systems~~BCS and their associated:

1. EACMS;
2. PACS; and
3. PCA

Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated:

1. EACMS;
2. PACS; and
3. PCA

SCI with ERC hosting High Impact BCS or Medium Impact BCS ~~with ERC~~ or their associated:

• PACS;
• EACMS; or
• PCA

Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated:

• PACS
• EACMS; or
• PCA | Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, a~~s~~t a minimum, each of the following types of events~~,~~ ~~(~~per system or Cyber A~~a~~sset or BES Cyber 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. |

| 4.3 | High Impact ~~BES Cyber Systems~~BCS and their associated:

1. EACMS;

2. PACS; and

3. PCA

Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated:

1. EACMS;

2. PACS; and

3. PCA

SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated:

• PACS;

• EACMS; or

• PCA

Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:

• PACS;

• EACMS; or

• PCA | ~~Where technically feasible, r~~Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system ~~or asset~~ 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 days or greater. |

CIP-007-76 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA Management Modules of SCI hosting High BCS or their associated: • EACMS; or • PCA	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, 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-007-76 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-007-76 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-67 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated:	Have a method(s) to enforce authentication of interactive user access, per system capability~~where technically feasible~~.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

	CIP-007-67 Table R5 – System Access Controls		
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated:	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).	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~~.

CIP-007-67 Table R5 – System Access Controls			
Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		

CIP-007-76 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated • PACS; • EACMS; or • PCA	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-007-76 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact BES Cyber SystemsBCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber SystemsBCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Change known default passwords, per system or Cyber Aasset 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 to the device.

CIP-007-76 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**

5.5	High Impact BES Cyber Systems and their associated:
	
	  1. EACMS;
	  2. PACS; and
	  3. PCA
	
	Medium Impact BES Cyber Systems and their associated:
	
	  1. EACMS;
	  2. PACS; and
	  3. PCA
	
	SCI hosting High or Medium Impact BCS or their associated:
	
	  • PACS;
	  • EACMS; or
	  • PCA
	
	Management Modules of SCI hosting High or Medium Impact BCS or their associated:
	
	  • PACS;
	  • EACMS; or
	  • PCA
		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 systemCyber Asset; 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.Cyber Asset.
			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-007-76 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated: • PACS;	~~Where technically feasible, F~~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 screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

	• EACMS; or • PCA		

CIP-007-76 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated:	~~Where technically feasible, either:~~ 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 showing how the system notified individuals after a determined number of unsuccessful login attempts.

	• PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		

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.

    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

~~Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	N/A	The Responsible Entity has implemented and documented processes for ~~Ports and Services~~ 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)	The Responsible Entity has implemented and documented processes for determining necessary System Hardening~~Ports and Services but~~, ~~where technically feasible,~~ but had one or more unneeded ~~logical~~ network accessible services ~~ports~~ enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has 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 implement or document one or more process(es) that included the applicable items in CIP-007-76 Table R1. (Requirement R1)
R2	The Responsible Entity has documented and implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for patch	The Responsible Entity has documented or implemented one or more	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	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 patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar	management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assetssystems. (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 vulnerabilities exposed by applicable security patches, did not	process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets 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 has one or more documented process(es) for evaluating	process(es) that included the applicable items in CIP-007-76 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 Cyber Assetssystems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision

R #	Violation Severity Levels (CIP-007-~~7~~6)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	days of the evaluation completion. (Requirement R2 Part 2.3)	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)	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)	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 but did not mitigate the	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels (CIP-007-76)			
	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)	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-007-76 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	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 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)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-76 Table R4. (Requirement R4)

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	at least every 15 calendar days but missed an 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)	but did not generate alerts 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 (where technically feasible and 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	OR 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-007-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more 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	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-76 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.

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			identification of the individuals with authorized 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	(Requirement R5 Part 5.1) 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.

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			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 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)	(Requirement R5 Part 5.4) OR 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

R #	Violation Severity Levels (CIP-007-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				interactive user access but did not technically or procedurally enforce password changes or 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~~,~~ ~~where technically feasible~~, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~See Project 2016-02 Virtualization 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.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-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	

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1.   This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement.   If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration

- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization

- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components

PSP

ESP

Applicability of CIP-007-6 R1, Part 1.2 for
Nonprogrammable Communication Components
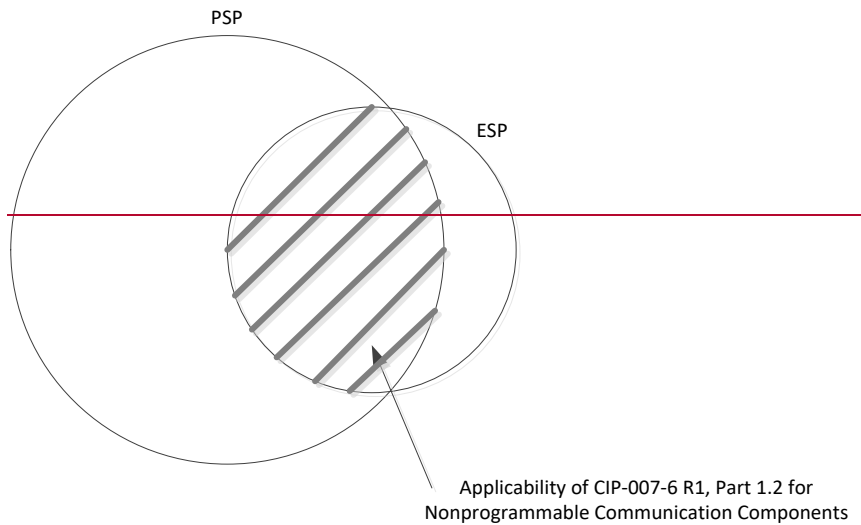
Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1.   The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system.   The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2.   Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3.   The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-

time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.

- Individual user account: An account used by a single user.

- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.

- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.

- Application account: A specific system account, with rights granted at the application level often used for access into a Database.

- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.

- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1   Reference the Requirement's rationale.

5.2   Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3   Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4.   Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5.   Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6   Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7   Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.