

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.¹
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

¹ In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

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 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated “Definitions of Terms Used in Version 5 CIP Cyber Security Standards,” which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the “Guidelines and Technical Basis” section of the Standard.

A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-5
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the 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 Facilities described in 4.2.2**
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Interchange Coordinator**
 - 4.1.6 **Load-Serving Entity that owns Facilities described in 4.2.1**
 - 4.1.7 **Reliability Coordinator**
 - 4.1.8 **Transmission Operator**
 - 4.1.9 **Transmission Owner**
 - 4.2. **Facilities:**
 - 4.2.1 **Load Serving Entity:** One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.
 - 4.2.2 **Distribution Provider:** One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:
 - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- 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.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

- 4.2.4.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
- 4.2.4.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
- 4.2.4.3** In nuclear plants, 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.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

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 a common subject matter.

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. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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 they feel necessary in their documented processes, but they 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.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. 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 applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **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.

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale for 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.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed.

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – 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 items in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems</p> <p>Medium Impact BES Cyber Systems with External Routable Connectivity</p> <p>Associated Physical Access Control Systems</p> <p>Associated Electronic Access Control or Monitoring Systems</p> <p>Associated Protected Cyber Assets</p>	<p>For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges or services where needed to handle dynamic ports.</p>	<p>Evidence may include, but is not limited to:</p> <ul style="list-style-type: none"> • Listings of the needed ports by Cyber Asset or class of Cyber Assets; • Listings of the listening ports on the Cyber Assets from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
<p>Reference to prior version: <i>CIP-007-4, R2.1 and R2.2</i></p>		<p>Change Description and Justification: <i>The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of ‘normal or emergency’ added no value and has been removed.</i></p>	

CIP-007-5 Table R1– Ports and Services			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	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.
Reference to prior version: NEW		Change Description and Justification: <i>In the March 18, 2010 FERC issued an order to approve NERC’s interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term “ports” in “ports and services” refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.</i>	

Rationale for 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.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the “release” date was. The current wording stated “document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades” there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

- R2.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 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 items in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A patch management program 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 applicable Cyber Assets that are updateable and for which a patching source exists.	Evidence must include documentation of a patch management program and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.
Reference to prior version: CIP-007, R3		Change Rationale: <i>The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also 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.</i>	

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in Part 2.1.	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 within 30 calendar days of availability.
Reference to prior version: CIP-007, R3.1		Change Rationale: <i>Similar to the current wording but added “from the source or sources identified in 2.1” to clarify the 30-day time frame.</i>	

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For applicable patches identified in Part 2.2, create a dated plan or revise an existing plan within 30 calendar days of the evaluation completion. The plan shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities exposed by each security patch and a timeframe to complete these mitigations.	Evidence may include, but is not limited to, 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 exposed by the security patch and a timeframe for the completion of these mitigations.
Reference to prior version: CIP-007, R3.2		Change Rationale: <i>The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity 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. The mitigation plan may, and in many cases will, consist of installing the patch. However, 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.</i>	

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For each plan created or revised in Part 2.3, implement the plan as created or revised within the timeframe specified in the plan, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • Records of the installation of the patch; • Records of implementation of vendor recommended mitigations; • Exports from automated patch management tools that provide installation date; • Verification of BES Cyber System Component software revision; • Registry exports that show software has been installed; or • Evidence that affected services have been disabled.
Reference to prior version: CIP-007, R3.2		Change Rationale: <i>Similar to the current wording but added “from the source or sources identified in Part 2.1” to clarify the 30-day time frame.</i>	

Rationale for 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.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset’s susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard “does not need to prescribe a single method...However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance...”

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

- R3.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*. [*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 items in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: <i>CIP-007-4, R4; CIP-007-4, R4.1</i>		Change Rationale: <i>See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.</i>	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Mitigate the threat of identified malicious code.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (e.g., quarantine, alert, etc.) to detected malicious code; or • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
Reference to prior version: <i>CIP-007-4, R4</i> <i>CIP-007-4, R4.1</i>		Change Rationale: <i>See the Summary of Changes.</i>	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections that use signatures or patterns at least once within 35 calendar days of each available signature or pattern release (this does not require use of every available release, but that for every release that is available, at least one update has occurred within 35 calendar days from that release), except for signature or pattern releases that the Responsible Entity documents as negatively affecting the Cyber Asset or BES Cyber System.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • Documentation showing the configuration of signature, or pattern updates for automated controls; or • Work logs showing the signature, or pattern updates for manual controls.
Reference to prior version: <i>CIP-007-4, R4; CIP-007-4, R4.2</i>		Change Rationale: <i>See the Summary of Changes. This part is written to ensure that signatures or patterns are updated within 35 days of release, but does not require installation of all releases so long as any given update occurs within 35 calendar days of each release. The part does not require update within 35 days of a particular release in cases where the Responsible Entity documents that the signature or pattern release negatively affects the Cyber Asset or BES Cyber System. Thirty-five Calendar days allows for a “once-a-month” frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.</i>	

Rationale for 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 immediate 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 and respond to audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor.”

The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

- R4.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 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 items in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. detected and logged failed access attempts at Electronic Access Points; 4.1.2. detected and logged successful and failed login attempts; 4.1.3. detected and logged malicious software; and 4.1.4. detected and logged malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required event types.
Reference to prior version: CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3		Change Description and Justification: <i>This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.</i>	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for security events that the Responsible Entity determines necessitate a real-time alert, that includes, as a minimum, each of the following types of events where technically feasible: <ul style="list-style-type: none"> 4.2.1. detected malicious activity; and 4.2.2. detected failure of 4.1 event logging. 	Evidence may include, but is not limited to paper or system-generated listing of security events which the Responsible Entity determined necessitate real-time alerts and paper or system generated list showing how real-time alerts are configured.
Reference to prior version: CIP-005-4, R3.2; CIP-007-4, R6.2		Change Description and Justification: <i>This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.</i>	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Activate a response to detected event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, documentation describing the response and its timing, or an attestation indicating that no such events occurred.
Reference to prior version: New Requirement		Change Rationale: <i>This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Misunderstandings with previous versions considered the failure of the security event monitoring and alerting system itself to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.</i>	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to: <ol style="list-style-type: none"> 1. security-related event logs from the past 90 days; 2. records of disposition of security-related event logs beyond 90 days up to the evidence retention period; and 3. paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: <i>CIP-005-4, R3.2; CIP-007-4, R6.4</i>		Change Rationale: <i>No substantive change.</i>	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events at a minimum every two weeks to identify undetected Cyber Security Incidents.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred.
Reference to prior version: CIP-005-4, R3.2; CIP-007-4, R6.5		Change Description and Justification: <i>Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.</i>	

Rationale for 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.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

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.

Summary of Changes (From R5): CIP-007-4, Requirements R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

- R5.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 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 items in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Enforce authentication of all user access, where technically feasible.	Evidence may include, but is not limited to, documentation describing how access is authenticated.
Reference to prior version: CIP-007-4, R5		Change Rationale: <i>The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase “that minimize the risk of unauthorized access” was removed and more appropriately captured in the rationale statement.</i>	

CIP-007-5 Table R5 – System Access Control			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of enabled or generic account types in use for the BES Cyber System.
Reference to prior version: <i>CIP-007-4, R5.2 and R5.2.1</i>		Change Rationale: <i>CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.</i>	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: <i>CIP-007-4, R5.2.2</i>		Change Rationale: <i>No significant changes. Added “authorized” access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.</i>	

CIP-007-5 Table R5 – System Access Control			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
5.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Change default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on Cyber Assets.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> Records of a procedure that passwords are changed when new devices are deployed; or Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: CIP-007-4, R5.2.1		Change Rationale: <i>The requirement for the “removal, disabling or renaming of such accounts where possible” has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.</i>	

CIP-007-5 Table R5 – System Access Control			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, 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 Cyber 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 Cyber Asset.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations by individuals that the procedurally enforced passwords meet the password parameters.
Reference to prior version: CIP-007-4, R5.3		Change Rationale: <i>CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.</i>	

CIP-007-5 Table R5 – System Access Control			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce password changes or an obligation to change the password at least once each calendar year, not to exceed 15 calendar months between changes.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations by individuals that the procedurally enforced passwords meet the password parameters.
Reference to prior version: CIP-007-4, R5.3.3		Change Rationale: <i>*This was originally Requirement R5.5.3, but moved to add “external routable connectivity” to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.</i>	

CIP-007-5 Table R5 – System Access Control			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
5.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Limit, where technically feasible, the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • 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.
Reference to prior version: New Requirement		Change Rationale: <i>Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.</i>	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

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 Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- 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 duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Same Day Operations	Medium	N/A	N/A		<p>The Responsible Entity did not have a documented process that included the applicable items in <i>CIP-007-5 Table R1</i>. (R1)</p> <p>OR</p> <p>The Responsible Entity had unneeded logical network accessible ports enabled.</p> <p>OR</p> <p>The Responsible Entity had no methods to protect unnecessary physical input/output ports used for network connectivity, console commands, or removable media.</p>
R2	Operations Planning	Medium	The Responsible Entity did not evaluate the	The Responsible Entity did not evaluate the	The Responsible Entity did not evaluate the	The Responsible Entity did not have a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 30 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	security patches for applicability within 45 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 45 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	security patches for applicability within 60 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 60 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	documented process that included the applicable items in <i>CIP-007-5 Table R2</i> . (R2) OR The Responsible Entity did not have a patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets or did not track for the release cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists. OR The Responsible Entity did not implement the plan as created or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						revised within the timeframe specified in the plan.
R3	Same Day Operations	Medium	Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 45 calendar days of each available signature or pattern release, but not within 35 calendar days. (3.3)	Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release, but not within 45 calendar days. (3.3).	Where signatures or patterns are used, the Responsible Entity did not update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release. (3.3).	The Responsible Entity did not have a documented process that included the applicable items in <i>CIP-007-5 Table R3</i> . (R3) OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not mitigate the threat of identified malicious code.
R4	Same Day Operations and	Medium	N/A	The Responsible Entity failed to identify and implement methods to	The Responsible Entity failed to activate a response to rectify the	The Responsible Entity did not have a documented process

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations Assessment			review a summarization of logged events every two weeks.	event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System security-related events for at least the last 90 consecutive days, where technically feasible.	that included the applicable items in <i>CIP-007-5 Table R4</i> . (R4) OR The Responsible Entity failed to implement methods to generate alerts for events that it determines to necessitate a real-time alert. OR The Responsible Entity failed to log detected events necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	Operations Planning	Medium	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared,	The Responsible Entity did not have a documented process that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					default, and other generic account types. OR The Responsible Entity failed to implement procedures to identify the individuals with authorized access to shared accounts.	<i>CIP-007-5 Table R5.</i> (R5) OR The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems. OR The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 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 is a requirement in CIP-005, Requirement R1 to protect the network and 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. 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

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. Stand alone 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 a low tier documents establishing the more detailed process followed for individual systems. Low 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 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, or those Cyber Assets that have no existing source of patches such as vendors that no longer exist.

2.2. Responsible Entities are to perform an assessment of security related patches within 30 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. 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. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system. 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. For those security related patches that are determined to be applicable, the Responsible Entity must create a dated plan within 30 days which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch. 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”. If the entity is going to install the patch, the plan can consist of a simple record that normal patch installation process from 2.1 will be followed and designate the date of the patch installation.

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, 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, portable storage media policies, 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 and should not require a TFE.

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.

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 requirement is written to handle two update frequency situations.

1) For those technologies that are providing very frequent updates (at most monthly but often daily or sometimes hourly), the updates applied to the applicable Cyber Assets should be no more than 35 calendar days old. In these instances, this is a 'maximum staleness' requirement. It does not require that every update within a 35 day period be applied, but that the currently installed update be no more than 35 days old.

2) For those technologies that provide less frequent updates that are more than 35 days, the requirements should be applied within 35 days of the last available update.

Testing of signature or pattern updates is not required. 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. Other Cyber Assets should have any updates 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 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, but the entity disables or neglects to enable that logging, it is a violation. 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
- 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. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the Cyber Asset and the logging system if the Cyber Asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs 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.

5.4. Where possible, any 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 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. 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.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account Password for a microprocessor relay, PLC, RTU, etc.	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During regularly scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	One year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	Two years or more