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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014

Description of Current Draft

This draft standard is being posted for an ~~initial~~ additional comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
~~First 45-Day Comment Period Opens~~	~~June 2014~~
Additional 45-Day Comment Period ~~(if necessary)~~	~~August~~ September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-2

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from 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 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 or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme 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-010-2:

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

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 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.

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require 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 Bulk Electric System. 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 applicability 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.
- **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. 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 with External Routable Connectivity.
- **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

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	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	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 4. EACMS; 5. PACS; and 6. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	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	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	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	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring. [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-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: **1.** EACMS; and **2.** PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table*.*

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	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	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	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	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 ~~is to address~~responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, ~~which require the standards~~ to address security-related issues associated with tools ~~specifically~~ used on a temporary basis for tasks such as~~for~~ data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To ~~that end~~mitigate the risks associated with such tools, the R~~r~~equirement R4 ~~goals are as follows~~is a new requirement developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

~~The SDT has incorporated~~Requirement R4 incorporates the concepts ~~of~~from other CIP requirements ~~from FERC-approved~~in CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. ~~While the requirements are similar, they are not to the same rigor of those found in CIP-007 protecting the permanent assets identified by an entity.~~ A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more documented ~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media* Protection~~ plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1, except under CIP Exceptional Circumstances. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable elements in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per element are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or

Removable Media~~Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table~~.

~~**CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection**~~			
~~**Part**~~	~~**Applicable Systems**~~	~~**Requirements**~~	~~**Measures**~~
~~4.1~~	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~• PCA~~	~~Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances.~~ ~~Authorization shall include:~~ ~~4.1.1. Users, individually or by group/role;~~ ~~4.1.2. Locations, individually or by group/role;~~ ~~4.1.3. Defined acceptable use; and~~ ~~4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or~~ ~~• A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.~~

~~CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection~~

~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~4.2~~	~~High Impact BES Cyber Systems and their associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ • ~~PCA~~	~~Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).~~	~~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 hardening, policies, verification of method(s) employed by vendors, etc.).~~
~~4.3~~	~~High Impact BES Cyber Systems and their associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ • ~~PCA~~	~~Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.~~	~~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 scanning techniques, verification of method(s) employed by vendors, etc.).~~
~~4.4~~	~~High Impact BES Cyber Systems and their associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ • ~~PCA~~	~~Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.~~	~~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.~~
~~4.5~~	~~High Impact BES Cyber Systems and their associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ • ~~PCA~~	~~Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use 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.~~

~~CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection~~

~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~4.6~~	~~High Impact BES Cyber Systems and their associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ • ~~PCA~~	~~Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4.~~ ~~For a modification that deviates from the state in Part 4.1.4, either:~~ • ~~Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or~~ • ~~Update Part 4.1.4.~~	~~An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.~~
~~4.7~~	~~High Impact BES Cyber Systems and associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ • ~~PCA~~	~~Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date.~~ ~~For security patches that are not up-to-date, take one of the following actions:~~ • ~~Apply the applicable patches;~~ • ~~Create a dated mitigation plan; or~~ • ~~Revise an existing mitigation plan.~~ ~~Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.~~	~~An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.~~

C. Compliance

1. Compliance Monitoring Process:

a. 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.

b. 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.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance ~~Violation~~ Investigations

Self-Reporting

Complaints ~~Text~~

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document the Removable Media elements according to CIP-010-2, Requirement R4, Attachment 1, element 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, element 1.1. (R4) ~~The Responsible~~	implement the Removable Media elements according to CIP-010-2, Requirement R4, Attachment 1, element 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement	implement mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, elements 1.2, 1.3, and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of security vulnerabilities or mitigation for the	Removable Media according to CIP-010-2, Requirement R4. (R4) ~~The Responsible Entity did not document or implement process(es) that collectively address the requirement parts as required by Requirement R4. (R4)~~ ~~OR~~ ~~The Responsible Entity did not use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability) as required by Requirement R4, Part 4.2. (4.2)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Entity has documented and implemented process(es) addressing authorization of use of Transient Cyber Assets, but failed to include one of the required items listed in 4.1.1 through 4.1.4. (4.1)~~	R4, Attachment 1, elements 1.2, 1.3, and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by Vendors or Contractors according to CIP-010-2, Requirement R4, Attachment 1, elements 2.1 and	introduction of malicious code for Transient Cyber Assets Owned or Managed by Vendors or Contractors according to CIP-010-2, Requirement R4, Attachment 1, elements 2.1 and 2.2. (R4) ~~The Responsible Entity has documented and implemented process(es) addressing authorization of use of Transient Cyber Assets, but failed to include three of the required items listed in 4.1.1 through 4.1.4. (4.1)~~ ~~OR~~ ~~The Responsible~~	~~The Responsible Entity did not use method(s) to detect malicious code on Removable Media prior to use on applicable systems as required by Requirement R4, Part 4.3. (4.3)~~ ~~OR~~ ~~The Responsible Entity did not mitigate the threat of detected malicious code for Transient Cyber Assets or Removable Media as required by Requirement R4, Part 4.4. (4.4)~~ ~~OR~~ ~~The Responsible Entity did not update signatures or patterns for those methods~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				2.2. (R4) ~~The Responsible Entity has documented and implemented process(es) addressing authorization of use of Transient Cyber Assets, but failed to include two of the required items listed in 4.1.1 through 4.1.4. (4.1)~~	~~Entity documented and implemented a process to evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 but did not take one of the actions required by Requirement R4, Part 4.6. (4.6)~~ ~~OR~~ ~~The Responsible Entity documented and implemented a process to evaluate Transient Cyber Assets within 35 calendar days prior to use but did not take one of the actions required by Requirement R4, Part 4.7. (4.7)~~	~~identified in Parts 4.2 and 4.3 that use signatures or patterns as required by Requirement R4, Part 4.5. (4.5)~~ ~~OR~~ ~~The Responsible Entity did not evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 as required by Requirement R4, Part 4.6. (4.6)~~ ~~OR~~ ~~The Responsible Entity did not evaluate Transient Cyber Assets within 35 calendar days prior to use as required by Requirement R4, Part~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~4.7. (4.7)~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-010-2 - Attachment 1

Required Elements for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the elements provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

1. Transient Cyber Asset(s) Owned or Managed by the Responsible Entity.

1.1. Transient Cyber Asset management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall specify:

1.2.1. Authorized users, either individually or by group or role;

1.2.2. Authorized locations, either individually or by group; and

1.2.3. Authorized uses, which shall be limited to what is necessary to perform business functions.

1.3. Security vulnerability mitigation: To mitigate security vulnerabilities (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate security vulnerabilities.

1.4. Introduction of malicious code mitigation: To mitigate the introduction of malicious code (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Risk of unauthorized use mitigation: To mitigate the risk of unauthorized use, each Responsible Entity shall use one or a combination of the following methods:

- Transient Cyber Asset resides within a location with restricted physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication;
- Theft recovery tools; or
- Other method(s) to mitigate the risk of unauthorized use.

2. Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors.

2.1 Security vulnerability mitigation: To mitigate security vulnerabilities (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Review of installed security patch(es);
- Review of security patching process used by the vendor or contractor;
- Review of other vulnerability mitigation performed by the vendor or contractor; or
- Other method(s) to mitigate security vulnerabilities.

2.2 Malicious code mitigation: To mitigate malicious code, each Responsible Entity shall use one or a combination of the following methods:

- Review of antivirus update level;
- Review of antivirus update process used by the vendor or contractor;
- Review of application whitelisting used by the vendor or contractor;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the vendor or contractor; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate security vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the vendor- or contractor-owned Transient Cyber Asset.

3. Removable Media

3.1. Removable Media authorization: For each individual or group of Removable Media, each Responsible Entity shall specify:

3.1.1. Authorized users, either individually or by group or role; and

3.1.2. Authorized locations, either individually or by group.

3.2. Malicious code mitigation: To mitigate malicious code, each Responsible Entity shall scan Removable Media outside of the BES Cyber System.

CIP-010-2 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Element 1.1: Examples of evidence for element 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) Owned or Managed by the Responsible Entity or part of a security policy.

Element 1.2: Examples of evidence for element 1.2 may include, but are not limited to,~~:~~ documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Transient Cyber Asset(s) Owned or Managed by the Responsible Entity. The documentation must identify the Transient Cyber Asset, individually or by group of Transient Cyber Asset(s) along with the authorized users, either individually or by group or role, the authorized locations, either individually or by group and the authorized uses associated with what is necessary to perform business functions.

Element 1.3: Examples of evidence for element 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate security vulnerabilities such as security patch management implementation, the use of live operating systems, system hardening practices or other method(s) to mitigate security vulnerability. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 1.4: Examples of evidence for element 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 1.5: Examples of evidence for element 1.5 may include, but are not limited to documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; method(s) of the theft recovery tools; or documentation of other method(s) to mitigate the risk of unauthorized use. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.1: Examples of evidence for element 2.1 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memorandums, electronic mail, policies or contracts from vendors or contractors that identify the security patching process or vulnerability mitigation performed by the vendor or contractor; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate security vulnerabilities for Transient Cyber Asset(s) Owned of Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.2: Examples of evidence for element 2.2 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed the antivirus update level; memorandums, electronic mail, system documentation, policies or contracts from vendors or contractors that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the vendor or contractor; evidence from change management systems, electronic mail or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.3: Examples of evidence for element 2.3 may include, but are not limited to documentation from change management systems, electronic mail, contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the vendor or contractor owned Transient Cyber Asset.

Element 3.1: Examples of evidence for element 3.1 may include, but are not limited to documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role and the authorized locations, either individually or by group.

Element 3.2: Examples of evidence for element 3.2 may include, but are not limited to documentation of the method(s) used to mitigate malicious code such as results of scans of the media, or documented confirmation by the entity that the media was deemed to be free of malicious code. Confirmation can be documented through email or within change management record(s).

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:

Baseline Configuration

The concept of establishing a Cyber Asset’s baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset’s baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks. Because of this, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas that are needed to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. These assets do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

~~This Requirement applies to any transient devices (i.e. Transient Cyber Assets and Removable Media) that will be connected temporarily to an applicable system. Examples of these devices include, but are not limited to:~~

- ~~Hardware/software ~~D~~d~~iagnostic test equipment

- ~~Hardware/software P~~packet sniffers
- ~~Hardware/software~~Equipment used for BES Cyber System maintenance
- ~~Hardware/software~~Equipment used for BES Cyber System configuration
- ~~Hardware/software~~Equipment used to perform vulnerability assessments

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, element 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and applications of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management. These are broken down as follows:

1. Transient Cyber Asset(s) Owned or Managed by the Responsible Entity
2. Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors
3. Removable Media

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to perform the security functions that the system is capable of doing. The use of this phrase is to eliminate the need for a technical feasibility exception when it is understood that the device cannot perform a function. Using the example of malicious code, many types of appliances are not capable of implementing antivirus software and therefore the software would not be required since it is not a capability of the device.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option that is most appropriate. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the device.

Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by the Responsible Entity

Element 1.1: Entities have a high level of control for the assets that they own or manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods.

Element 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct ownership or management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks, and approved network interfaces (e.g. wireless including near field communication or Bluetooth and wires connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

~~Transient Cyber Assets can be in the form of a laptop, desktop, or tablet. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~This requirement does not cover hardware/software components that may support information system maintenance yet are a part of the system, for example the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of a switch.~~

~~Requirement Parts 4.1, 4.3, 4.6, and 4.7 refer to the term "prior to use" related to when specific actions must occur. For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. For example, a technician would need to have a laptop evaluated only once according to Part 4.6 when working in the same PSP. The technician would not need to have the evaluation performed each time it connects to a different Cyber Asset.~~

~~**Requirement Part 4.1:**~~

~~Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets. This allows entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection. The Transient Cyber Assets~~

~~may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:~~

~~1.~~ ~~User(s), individually or by group/role, allowed to use Transient Cyber Assets. This is intended to provide assurance around who has physical proximity to the Transient Cyber Assets. These user(s) must have authorized electronic and unescorted physical access to the applicable system in accordance with CIP-004.~~

~~2.~~ ~~Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group/role of locations. Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. It may be reasonable to have separate Transient Cyber Assets for each impact level.~~

~~3.~~ ~~The intended or approved use of each Transient Cyber Asset. Activities not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals on the activities or uses that are not allowed (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).~~

~~4.~~ ~~The operating system, firmware, and intentionally installed software. All of this information may not be available or relevant to each Transient Cyber Asset. Having this information facilitates the review in Part 4.6. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The Standard Drafting Team does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included.~~

~~CAUTION:~~ Entities should exercise caution when using Transient Cyber Assets and ensure they do not have ~~wireless or Bluetooth~~ features enabled (e.g. wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Element 1.3: Entities are to document and implement their process(es) to mitigate security vulnerabilities through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in security vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how their Transient Cyber Asset(s) will be used. It is possible for an entity to have their Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike, CIP-007, R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating customer live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate security vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet security vulnerability mitigation.

Element 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns provides flexibility just as with security patching, to manage their Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, it is possible that entities can choose for devices that do not regularly connect to receive scheduled updates, to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate from the Transient Cyber Asset to the BES Cyber Asset of BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the introduction of malicious code.

Element 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks of unauthorized use to the Transient Cyber Asset.

- Transient Cyber Asset resides within a location with restricted physical access. The intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location that manages unauthorized physical access to the device.
- Full disk encryption with authentication is an option that can be used to protect a Transient Cyber Asset from unauthorized physical access. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents anything being read from the hard disk until the user has confirmed they have the correct password or other credentials.
- Multi-factor authentication is used to ensure the identity of the person accessing the device.
- Theft recovery tools that can be used to remotely wipe or lockout systems if they are stolen or lost.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of unauthorized use.

~~Requirement Parts 4.2, 4.3, 4.4, and 4.5:~~

~~Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.~~

~~It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.~~

~~For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.~~

~~For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.~~

~~Requirement Parts 4.6 and 4.7:~~

~~Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.~~

~~Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.~~

~~Requirement Parts 4.2, 4.3, 4.4, and 4.5:~~

~~Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of~~

~~connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.~~

~~It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.~~

~~For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.~~

~~For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.~~

~~Requirement Parts 4.6 and 4.7:~~

~~Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.~~

~~Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.~~

Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors

The attachment also recognizes the lack of control for Transient Cyber Assets that are owned or managed by vendors or contractors. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with vendors and contractors to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department Of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Elements from the procurement language may unify vendor and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP Program elements may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the vendor's support. Entities should consider the elements of the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Element 2.1: Entities are to document and implement their process(es) to mitigate security vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the vendor or contractor managed Transient Cyber Asset to determine whether the security patch level of the device is adequate to mitigate the risk of security vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the vendor or contractor security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of security vulnerabilities to applicable systems.
- Conduct a review of other processes that the vendor or contactor uses to mitigate the risk of security vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate security vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of security vulnerabilities

Element 2.2: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the vendor or contactor to ensure that their processes are adequate to the Responsible Entity to reduce the risk of introducing malicious software to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of application whitelisting used by the vendor or contractor to reduce the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the vendor or contractor to ensure that unnecessary ports, services, applications, etc have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Element 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the vendor or contractor owned Transient Cyber Asset. The intent of this element is to ensure that after conducting the selected review from elements 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entities security posture, the vendor or contractor is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement 4 Attachment 1 Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Element 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Element 3.2: Entities are to document and implement their process(es) to mitigate malicious code through the use of scanning the Removable Media before it is connected to a BES Cyber Asset. The scanning is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.