Standard Development Timeline

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

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed of modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

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

2. **Number:** CIP-010-54

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting ~~BES Cyber Systems~~BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-54:

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

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

~~4.2.3.2.~~ 4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~ 4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~ 4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

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

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

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for Project 2019-03~~.

~~**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 BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

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

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

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 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

R1. Each Responsible Entity shall implement one or more documented process(es) to manage changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-54 Table R1 – Security 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-010-54 Table R1 – Security Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS~~ES Cyber Systems~~ and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact BCS~~ES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Develop a baseline configuration, individually or by group, which shall include the following items:~~ Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007. For those changes: 1.1.1. Authorize the changes; and ~~Operating system(s) (including version) or firmware where no independent operating system exists;~~ 1.1.2. Verify the required cyber security controls remain implemented as required as a part of the change. Changes to software include the	Examples of evidence may include, but are not limited to, a documented process that controls intended changes to settings that may weaken cyber security controls in CIP-005 and CIP-007, such as: • Operating system (OS) software; • Firmware; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity

CIP-010-54 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		installation, removal, or update of operating system, firmware, commercial and custom software, and security patches. ~~Any commercially available or open-source application software (including version) intentionally installed;~~ ~~1.1.2. Any custom software installed;~~ ~~1.1.3. Any logical network accessible ports; and~~ ~~1.1.4. 1.1.5. Any security patches applied.~~	control between systems with different impact ratings; • Changes to configurations or settings for an ESP between systems with different impact ratings; • Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or • Any other configuration or setting determined by the Responsible Entity. (1.1.1.) • A change request record and associated authorization for applicable changes; or • Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.2.) • A list of cyber security controls verified along with the dated results; or

CIP-010-54 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• A dated output from cyber security tools such as a vulnerability scanner. • ~~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.~~
~~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:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. 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-010-54 Table R1 – Security 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.~~
1.25	High ~~I~~impact BCSES Cyber Systems	~~Where technically feasible, for each change that deviates from the existing baseline configuration:~~ 1.25.1. Prior to implementing an~~y~~	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

CIP-010-54 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		intended change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production 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 the configuration of required cyber security controls in CIP-005 and CIP-007~~ are not adversely affected~~ remain implemented as required; and 1.2~~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.	differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.
1.3~~6~~	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated:	Prior to ~~a change~~the installation of operating systems, firmware, software,	An example of evidence may include, but is not limited to a change request

CIP-010-54 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	or software patches ~~that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5,~~ and when the method to do so is available to the Responsible Entity from the software source: 1.~~3~~6.1. Verify the identity of the software source; and 1.~~3~~6.2. Verify the integrity of the software obtained from the software source.	record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to ~~the baseline change~~ installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-54 Table R2 – Security 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-010-54 Table R2 – Security Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R2 – Security Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Methods to ~~M~~monitor at least once every 35 calendar days for unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007, per system capability. ~~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 or records from a system that is monitoring ~~the configuration~~for unauthorized changes along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-53 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-010-53 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~l~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	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-010-54 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BES Cyber Systems SCI supporting an Applicable System in this Part	~~Where technically feasible, a~~At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production 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-010-54 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High ~~i~~impact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances. ~~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: • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) ~~, a~~that documents ~~listing~~ the date of the assessment performed prior to becoming a new Applicable System. ~~the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.~~

CIP-010-54 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High ~~l~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	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 e~~Examples of evidence may include, but ~~is~~are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • ~~, a d~~Documentation 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).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, ~~and~~ associated ~~Protected Cyber Assets~~PCAs and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[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~~TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for ~~Transient Cyber Assets~~TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use ~~Transient Cyber Asset~~TCA(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~~TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) 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 applicable 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 applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~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's change management process(es) does not include one of the required items listed in 1.1.1 through 1.1.3. (Part 1.1); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management	~~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)~~ ~~OR~~ The Responsible Entity ~~has~~ change management ~~a~~ process(es) did not include the two required items listed in 1.1.1 through 1.1.3. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR	The Responsible Entity ~~has not~~neither documented nor implemented any ~~configuration~~ change management process(es) that include required items in Part 1.1 through Part 1.3. (Requirement 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 requires authorization and documentation of changes that deviate from the~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) ~~as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)~~	~~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 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~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~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)~~ ~~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 #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~OR~~ ~~The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)~~
R2.	N/A	N/A	The Responsible Entity did not document nor implemented a process(es) with methods to monitor for unauthorized changes at least once every 35 calendar days. (Part 2.1); OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1);~~N/A~~	The Responsible Entity ~~has not~~ neither documented nor implemented a process(es) with methods to monitor for, ~~investigate, and document detected unauthorized changes to the baseline~~ at least once every 35 calendar days and neither documented nor investigated detected unauthorized changes. (Part 2.1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	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, since the last assessment on one of its ~~a~~Applicable Systems ~~BES Cyber Systems~~. (Part 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 ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	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, since the last assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 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 ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	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, since the last assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 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 ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	The Responsible Entity ~~has~~ did not implement~~ed~~ any vulnerability assessment processes for one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Requirement R3) OR 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 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 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~~of a Cyber System prior to it becoming an ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				each of its ~~a~~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. (Part 3.4)
R4.	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not manage its Transient Cyber Asset(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~ did not implement the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not authorize its ~~Transient Cyber Asset~~TCA(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity did not ~~failed to~~ document or implement one or more plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media according to ~~CIP-010-4,~~ Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Removable Media, but failed to~~did not document the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document authorization for ~~Transient Cyber Assets~~ TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (Requirement R4)	~~Removable Media plan, but failed to~~did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~ did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according	~~Removable Media, but failed to~~ did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCAs managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCAs managed by a party other than the Responsible Entity according	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections ~~2.~~1.3, ~~2.2~~1.4, and ~~2.3.~~1.5. (Requirement R4)	to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for Project 2019-03~~.
- CIP-010-54 Technical Rationale

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	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-4 - Attachment 1
Required Sections for Plans for Transient Cyber Assets and Removable Media

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

Section 1. ~~Transient Cyber Asset~~TCA(s) Managed by the Responsible Entity.

1.1. ~~Transient Cyber Asset~~TCA Management: Responsible Entities shall manage ~~Transient Cyber Asset~~TCA(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~~TCA Authorization: For each individual or group of ~~Transient Cyber Asset~~TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

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

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per ~~Transient Cyber Asset~~TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- ~~Live operating system and software executable only from read-only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- Application whitelisting; or

- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of ~~Transient Cyber Asset~~TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. ~~Transient Cyber Asset~~TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per TCA~~Transient Cyber Asset~~ capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of ~~O~~other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code~~use of live operating system and software executable only from read-only media~~;
- Review of system hardening used by the party; or
- Review of ~~O~~other method(s) to mitigate malicious code.

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code ~~to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets~~, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ~~using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets~~; and

3.2.2. Mitigate the threat of detected malicious code ~~on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~.

CIP-010-4 - Attachment 2

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

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

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution~~live operating systems from read-only media~~, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. 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~~methods to maintain the known good state of the OS and all software, or system hardening practices. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software ~~processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code~~, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.5: Examples of evidence for Section 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; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 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); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software ~~use of live of operating systems or system hardening performed~~ by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 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.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.