

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 ~~final-second~~ draft of ~~the~~ proposed standard ~~for formal 10-day comment period~~.

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
4560 -day formal comment period with ballot	January 21– February <u>March 22</u> , 2021
<u>45-day formal comment period with ballot</u>	<u>June 30 – August 13, 2021</u>

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 329 – September 16 <u>October 11</u> , 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Change Management and Vulnerability Assessments
2. **Number:** CIP-010-5
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 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-010-5:

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

4.2.3.2. Cyber ~~s~~Systems associated with communication links ~~logically isolated from, but not providing logical isolation for, BES Cyber~~

~~Systems or SC~~between discrete Electronic Security Perimeters (ESP).

- 4.2.3.3. Cyber ~~s~~Systems, associated with communication links, ~~between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that~~Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.
 - 4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
 - 4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
 - 4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.
- 4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~for~~ part applies. ~~This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~
5. **Effective Date:** See “Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan.”

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –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-010-5 Table R1 –Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems <u>(BCS)</u> and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems<u>BCS</u> and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p><u>SCI identified independently supporting an Applicable System above</u></p> <p><u>SCI hosting High or Medium Impact BCS or their associated:</u></p> <ul style="list-style-type: none"> • PACS; • EACMS; or 	<p>Authorize changes to:</p> <ol style="list-style-type: none"> 1.1.1. Operating system(s) <u>(OS)</u>; or firmware <u>where no independent OS exists</u>; or images used to derive operating systems; or firmware; 1.1.2. Commercially available or open-source application software, including <u>application containers</u> Self-Contained Applications; 1.1.3. Custom software installed, including Self-Contained Applications <u>containers</u>; and 1.1.4. Any logical network accessible services, ports (or logical ports <u>services</u> if unable to determine service <u>ports</u>); Security patches applied; 	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • <u>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.</u> • <u>Documentation of authorization for cyber security patch implementation.</u>

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
	<ul style="list-style-type: none"> ● PCA <p>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> ● PACS; ● EACMS; or ● PCA 	<p>SCI configuration that:</p> <ul style="list-style-type: none"> Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI; Enforces logical isolation between systems with different impact ratings hosted on SCI; Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or Enables or disables SCI services. 	
<u>1.2</u>	<p><u>SCI identified independently supporting an Applicable System from Part 1.1.</u></p>	<p><u>Authorize changes to SCI configuration that:</u></p> <ul style="list-style-type: none"> <u>1.2.1. Controls sharing of CPU or memory between systems with different impact ratings, including non-CIP Systems, hosted on SCI; and</u> <u>1.2.2. Enforces an ESP between systems with different impact ratings, including non-CIP Systems, hosted on SCI.</u> 	<p><u>Examples of evidence may include, but are not limited to:</u></p> <ul style="list-style-type: none"> ● <u>Documentation of authorization for changes to configuration of host affinity control between systems with different impact ratings;</u> ● <u>Documentation of authorization for changes to policies or configurations for an ESP between systems with different impact ratings.</u>

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
1.23	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>SCI identified independently supporting an Applicable System above</p> <p>SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> ● PACS; ● EACMS; or ● PCA <p>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> ● PACS; ● EACMS; or 	<p>For each change to the items listed in Part 1.1:</p> <p>1.23.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;</p> <p>1.23.2. Following the change, verify that required cyber security controls determined in 1.23.1 are not adversely affected; and</p> <p>1.23.3. Document the results of the verification.</p>	<p>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.</p>

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
	<ul style="list-style-type: none"> ● PCA 		
1.34	<p>High Impact BCS</p> <p>SCI identified independently supporting an Applicable System above SCI hosting High Impact BCS</p>	<p>For each change to the items listed in Part 1.1 <u>or Part 1.2</u>, per system capability:</p> <p>1.34.1. Prior to implementing any change 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 to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and</p> <p>1.34.2. 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</p>	<p>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 the date of the test.</p>

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
		production environments.	
1.45	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> EACMS; and PACS <p>Medium Impact BCS and their associated:</p> <ol style="list-style-type: none"> EACMS; and PACS <p>SCI identified independently supporting an Applicable System above SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.</p> <p>Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.</p> <p>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 1.45: (1) the actual terms and conditions of a procurement contract; and (2) vendor</p>	<p>Prior to a change associated with Requirement Parts 1.1.1, and 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:</p> <ol style="list-style-type: none"> 1.45.1. Verify the identity of the software source; and 1.45.2. Verify the integrity of the software obtained from the software source. 	<p>An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.</p>

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
	performance and adherence to a contract.		

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change 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-010-5 Table R2 – Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Change Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <u>SCI identified independently supporting an Applicable System above</u>	Monitor at least once every 35 calendar days for unauthorized changes to the items described listed in Requirement R1, Part 1.1. <u>and Part 1.2.</u> 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.

- R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 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-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>SCI identified independently supporting an Applicable System above</p> <p>SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> ● PACS; ● EACMS; or ● PCA <p>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> ● PACS; ● EACMS; or ● PCA 	<p>At least once every 15 calendar months, conduct a paper or active vulnerability assessment.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> ● 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-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems</p> <p><u>SCI identified independently supporting an Applicable System above</u></p> <p>SCI hosting High Impact BCS.</p> <p>Management Modules of SCI hosting High Impact BCS.</p>	<p>At least once every 36 calendar months, per system capability:</p> <p>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; and</p> <p>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.</p>	<p>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.</p>

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PCA <p>SCI identified independently supporting an Applicable System above SCI hosting High Impact BES Cyber Systems or their associated: PACS; EACMS; or PCA Management Modules of SCI hosting High Impact BCS or their associated: EACMS; or PCA</p>	<p>Prior to becoming a new Applicable System, Pperform an active vulnerability assessment <u>of the new Applicable System, prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability, except for:</u></p> <ul style="list-style-type: none"> • for CIP Exceptional Circumstances, like <u>replacements of the same type of Cyber System with a or deployments using a previously assessed configuration of the previous or other existing Cyber System; or</u> <u>CIP Exceptional Circumstances.</u> –The production environment does not include devices being actively remediated and logically isolated. 	<p>An example of evidence may include, but is not limited to:</p> <ul style="list-style-type: none"> <u>The output of any tools used to perform the assessment, or</u> <u>Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.)</u> <p>that documents the date of the assessment performed prior to becoming a new Applicable System BES Cyber System or SCI. a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.</p>

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.4	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p><u>SCI identified independently supporting an Applicable System above</u></p> <p>SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • PACS; • EACMS; or • PCA <p>Management Modules of SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • PACS; • EACMS; or PCA 	<p>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.</p>	<p>An example of evidence may include, but is not limited to:</p> <ul style="list-style-type: none"> • Reports or logs from SCI mechanisms and remediation of VCAs at instantiation; or of Management System actions, or • <u>Documentation</u> 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 SCI and Protected Cyber Assets,~~ 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, that except for use on low impact BCS or SCI supporting only low impact BCS(s) 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 Asset~~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 Asset~~TCAs 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.	<p>The Responsible Entity has documented and implemented a change management authorization process(es) that includes only four or more of the required items listed in 1.1.1 through 1.1.46. (Requirement R1 Part 1.1)</p>	<p>The Responsible Entity has documented and implemented a change management authorization process(es) that includes only three of the required items listed in 1.1.1 through 1.1.46. (Requirement R1 Part 1.1)</p>	<p>The Responsible Entity has documented and implemented a change management authorization process(es) that includes only two of the required items listed in 1.1.1 through 1.1.46. (Requirement R1 Part 1.1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a change authorization process(es) that includes only one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2)</p> <p>OR</p> <p>The Responsible Entity has a process as specified in Part 1.54 to verify the identity of the software source (1.54.1) but does not have a process as specified in Part 1.54 to verify the integrity of the</p>	<p>The Responsible Entity has not documented or implemented any change management authorization process(es). (Requirement R1)</p> <p>OR</p> <p>The Responsible Entity has documented and implemented a change management authorization process(es) that includes only one of the required items listed in 1.1.1 through 1.1.46. (Requirement R1 Part 1.1)</p> <p>OR</p> <p>The Responsible Entity does not have a change management authorization process(es) that requires authorization of changes to items listed in 1.1.1-1.1.46. (Requirement R1 Part 1.1)</p> <p>OR</p>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.54.2)</p>	<p><u>The Responsible Entity does not have a change authorization process(es) that requires authorization of changes to items listed in 1.2.1 to 1.2.2 (Requirement R1 Part 1.2)</u></p> <p>OR</p> <p>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 configuration. (Requirement R1 Part 1.32.1)</p> <p>OR</p> <p>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 configuration but did not verify and</p>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>document that the required controls were not adversely affected following the change. (Requirement R1 Part 1.32.2 & Part 1.32.3)</p> <p>OR</p> <p>The Responsible Entity does not have a process for testing changes prior to implementing a change to the configuration. (Requirement R1 Part 1.43.1)</p> <p>OR</p> <p>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. (Requirement R1 Part 1.43.2)</p> <p>OR</p> <p>The Responsible Entity does not have a process as</p>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>specified in Part 1.54 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. (Requirement R1 Part 1.54)</p>
R2.	N/A	N/A	N/A	<p>The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.1. at least once every 35 calendar days. (Requirement R2 Part 2.1)</p> <p><u>OR</u></p> <p><u>The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the</u></p>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<u>items described in Requirement R1, Part 1.2. at least once every 35 calendar days. (Requirement R2 Part 2.1)</u>
R3.	<p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Requirement R3 Part 3.1)</p> <p>OR</p> <p>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</p>	<p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Requirement R3 Part 3.1)</p> <p>OR</p> <p>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</p>	<p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Requirement R3 Part 3.1)</p> <p>OR</p> <p>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</p>	<p>The Responsible Entity has not implemented any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more</p>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	less than 39 months, since the last active assessment on one of its A pplicable S ystems. (Requirement R3 Part 3.2)	less than 42 months, since the last active assessment on one of its A pplicable S ystems. (Requirement R3 Part 3.2)	less than 45 months, since the last active assessment on one of its A pplicable S ystems. (Requirement R3 Part 3.2)	<p>documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable systems.(Requirement R3 Part 3.2)</p> <p>OR</p> <p>The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its Applicable Systems, but did not perform the active vulnerability assessment of <u>a Cyber System prior to it becoming an its Applicable Systems.</u> (Requirement R3 Part 3.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented vulnerability</p>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessment processes for each of its A pplicable S ystems, 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. (Requirement R3 Part 3.4)
R4.	<p>The Responsible Entity documented its plan(s) for Transient Cyber AssetTCA(s) and Removable Media, but failed to manage its Transient Cyber AssetTCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.1. (Requirement R4 Part R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for</p>	<p>The Responsible Entity documented its plan(s) for Transient Cyber AssetTCA(s) and Removable Media, but failed to implement the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for</p>	<p>The Responsible Entity documented its plan(s) for Transient Cyber AssetTCA(s) and Removable Media, but failed to authorize its Transient Cyber AssetTCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for</p>	<p>The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber AssetTCA(s) and Removable Media according to CIP-010-5, Requirement R4. (R4)</p>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>Transient Cyber Asset TCAs and Removable Media, but failed to document the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Asset TCAs and Removable Media, but failed to document authorization for Transient Cyber Asset TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)</p>	<p>Transient Cyber Asset TCAs and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Asset TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Asset TCAs and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Asset TCAs managed by a party other than the</p>	<p>Transient Cyber Asset TCAs and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Asset TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Asset TCAs and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Asset TCAs managed by a party other than the</p>	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Responsible Entity according to CIP-010-5, 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 ~~Virtualization~~ Modification to CIP Standards Implementation Plan.”.
- CIP-010-5 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	10/18/18	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	
5	TBD	Virtualization modifications	

CIP-010-5 - 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 (TCA) 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~~(TCAs), 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~~BCS, 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~~(TCAs), 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 that mitigates the risk of introduction of malicious code~~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 that mitigates the risk of introduction of malicious code;

- 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(s)~~TCAs:

- 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(s)~~TCAs 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 ~~Transient Cyber Asset~~TCA 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 ~~Q~~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 ~~Q~~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 ~~to 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-010-5 - 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(TCAs)~~. This can be included as part of the ~~Transient Cyber AssetTCA~~ plan(s), part of the documentation related to authorization of ~~Transient Cyber Asset(TCAs)~~ 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(TCAs)~~ 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, ~~controls to maintain the known good state of the OS and all software~~~~the use of 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 ~~controls to maintain the known good state of the OS and all software~~~~system hardening practices~~. If a ~~Transient Cyber AssetTCA~~ 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 AssetTCA~~ 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 AssetTCA~~ 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(TCAs)~~ 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(TCAs)~~ 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.