NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-010-5 – Cyber Security – Configuration Change Management and Vulnerability Assessments

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Name of Registered Entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		
R4	X	*	X	X		X			X	X		

*CIP-010-5 is only applicable to DPs that own certain UFLS, UVLS, RAS, protection systems, or cranking paths. See CIP-010-5 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest version of the Reliability Standards, approved by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request from the registered entity additional evidence that is not included in this RSAW. Additionally, this RSAW may include excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1* – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Accet (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include the authorization of changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.
	Verify that the Responsible Entity has implemented one or more processes that include the authorization of changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.

Auditor Notes:

R1 Part 1.2

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS	1.2.1 Prior to implementing any 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, to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.2. 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 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, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include: 1.2.1 Prior to implementing any 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, to ensure that required cyber security controls in CIP-005 and CIP- 007 are not adversely affected; and 1.2.2 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.
	Verify that the Responsible Entity has implemented one or more processes that include: 1.2.1 Prior to implementing any 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, to ensure that required cyber security controls in CIP-005 and CIP- 007 are not adversely affected; and 1.2.2 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.

Auditor Notes:

R1 Part 1.3

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact 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.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	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 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.3
This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include: Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.
	Verify that the Responsible Entity has implemented one or more processes that include: Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.

Auditor Notes:

R1 Part 1.4

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include verification that the behavior(s) of the altered cyber security controls were not adversely affected as a part of the changes authorized per Part 1.1.
	Verify that the Responsible Entity has implemented one or more processes that include verification that the behavior(s) of the altered cyber security controls were not adversely affected as a part of the changes authorized per Part 1.1.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber System and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.
	Verify the Responsible Entity implemented one or more processes to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.

Auditor Notes:

R3 Supporting Evidence and Documentation

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.

R3 Part 3.1

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes for conducting a paper or active vulnerability assessment at least once every 15 calendar months.
	For each Applicable System, verify the Responsible Entity conducted a paper or active vulnerability assessment at least once every 15 calendar months.

Auditor Notes:

R3 Part 3.2

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	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; 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes to: 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 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.
	Verify the Responsible Entity implemented one or more processes to: 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 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.
	For each Applicable System, per system capability, verify an active vulnerability assessment was conducted at least once every 36 calendar months, in accordance with 3.2.1; and results of testing was documented, in accordance with 3.2.2.
	If a system is incapable of conducting an active vulnerability assessment at least once every 36 months, verify that compensating measures are implemented.

Auditor Notes:

R3 Part 3.3

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS 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 or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of 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.) that documents the date of the assessment performed prior to becoming a new Applicable System.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes for performing an active vulnerability assessment on each new Applicable System, prior to it becoming a new Applicable System, except for CIP Exceptional Circumstances and like replacements of the same type with a baseline configuration that models an existing baseline configuration of the previous or other existing Applicable System.
	Verify the Responsible Entity implemented one or more processes for performing an active vulnerability assessment on each new Applicable System, prior to it becoming a new Applicable System, except for CIP Exceptional Circumstances and like replacements of the same type with a baseline configuration that models an existing baseline configuration of the previous or other existing Applicable System.
	If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R3 Part 3.4

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS 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.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • 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).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes to 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.
	For each Applicable System, for each assessment conducted according to Parts 3.1, 3.2, and 3.3, verify the results of the assessment were documented.
	For each Applicable System, for each assessment conducted according to Parts 3.1, 3.2, and 3.3, for any vulnerabilities identified, verify: 1. An action plan to remediate or mitigate the identified vulnerabilities was created or modified; 2. the action plan includes a planned date of completion; 3. the action plan includes the execution status of any remediation or mitigation action items; 4. the status of the action plan, if the planned date of completion has been exceeded; and 5. the completion of the action plan, if the action plan status is complete.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, 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 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 TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use 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 TCA(s) or Removable Media.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R4

This section to be completed by the Compliance Enforcement Authority

	Section 1. For TCA(s) managed by the Responsible Entity:
	Verify that the Responsible Entity has documented at least one plan, as specified in Attachment 1, for TCA(s) that includes: 1. TCA management; 2. TCA authorization; 3. software vulnerability mitigation; 4. introduction of malicious code mitigation; and 5. unauthorized use mitigation.
	Verify that the Responsible Entity has implemented its plan(s) to manage 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, or (3) a combination of both (1) and (2) above.
	For each individual or group of TCA(s), verify the Responsible Entity authorizes: 1. Users, either individually or by group or role; 2. Locations, either individually or by group; and 3. Uses, which shall be limited to what is necessary to perform business functions.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability): • Security patching, including manual or managed updates; • System hardening; or • Other method(s) to mitigate software vulnerabilities. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability): • Live operating system and software executable only from read-only media; • Antivirus software, including manual or managed updates of signatures or patterns; • Application whitelisting; or • Other method(s) to mitigate the introduction of malicious code. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of 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. For TCA(s) managed by a party other than the Responsible Entity:	
	Verify that the Responsible Entity has documented at least one plan, as specified in Attachment 1, for TCA(s) managed by a party other than the Responsible Entity that includes: 1. Software vulnerability mitigation; 2. introduction of malicious code mitigation; and 3. determination of additional mitigation actions, as necessary.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per 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 • other method(s) to mitigate software vulnerabilities. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating malicious code (per 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 use of live operating system and software executable only from read-only media; • review of system hardening used by the party; or • Review of other method(s) to mitigate the risk of introduction of malicious code. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2: 1. Verify that the Responsible Entity determined whether any additional mitigation actions are necessary. 2. If any additional mitigation actions were necessary, verify that such actions were implemented prior to connecting the TCA.

Section 3. For Removable Media:	
	Verify that the Responsible Entity has documented at least one plan, as specified in Attachment 1, for Removable Media that includes: 1. Removable Media authorization; and 2. malicious code mitigation.
	Verify the Responsible Entity authorized, for each individual or group of Removable Media: 1. Users, either individually or by group or role; and 2. locations, either individually or by group.
	Verify the Responsible Entity has implemented method(s) to detect malicious code on Removable Media prior to connecting and mitigated the threat of detected malicious code.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-010-5 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

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. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage 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, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of 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 TCA (per TCA capability):

- Security patching, including manual or managed updates;
- 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 risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; 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 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. 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 TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of other vulnerability mitigation performed by the party; or
- Review of 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 the risk of introduction of malicious code (per 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 system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of 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 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, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting; and

3.2.2. Mitigate the threat of detected malicious code.

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 TCA(s). This can be included as part of the TCA plan(s), part of the documentation related to authorization of 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 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 the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, 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, system hardening practices or other method(s) to mitigate the risk of 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, methods to maintain the known good state of the OS and all software, or system hardening practices. If a 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 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, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA 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 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; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that document a

review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that document a review of 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; 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 TCA(s) managed by a party other than the Responsible Entity. If a 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 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, and system hardening 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 TCA(s) managed by a party other than the Responsible Entity. If a 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 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 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.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFTv1	02/28/2024		Initial Draft