NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-010-2 – 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:	Registered name of 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	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		
R3	X	X	X	X	X				X			X	X		
R4	X	X	X	X	X				X			X	X		

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 approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides 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 reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes 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			
P1.1			
P1.2			
P1.3			
P1.4			
P1.5			
R2			
P2.1			
R3			
P3.1			
P3.2			
P3.3			
P3.4			
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) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

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

R1 Part 1.1

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1 Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2 Any commercially available or open-source application software (including version) intentionally installed; 1.1.3 Any custom software installed; 1.1.4 Any logical network accessible ports; and 1.1.5 Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

Registered Entity Response (Required):
Question: Is R1 Part 1.1 applicable to this audit? □ Yes □ No
If “No,” why not?
□ This entity is not responsible for compliance for any of the systems listed in the “Applicable Systems” column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, 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 development of a baseline configuration for each Applicable System.
	For each Applicable System, verify the above process(es) collectively include all of the following: 1. Operating system(s) (including version) or firmware where no independent operating system exists; 2. any commercially available or open-source application software (including version) intentionally installed; 3. any custom software installed; 4. any logical network accessible ports; and 5. any security patches applied.
	Verify the entity has a baseline configuration for each Applicable System, individually or by group, which includes: 1. Operating system(s) (including version) or firmware where no independent operating system exists; 2. any commercially available or open-source application software (including version) intentionally installed; 3. any custom software installed; 4. any logical network accessible ports; and 5. any security patches applied.

Auditor Notes:

____

R1 Part 1.2

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

Registered Entity Response (Required):
Question: Is R1 Part 1.2 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity documented one or more processes to authorize and document changes that deviate from the existing baseline configuration.
	For each Applicable System, verify the entity authorized and documented changes that deviate from the existing baseline configuration.

Auditor Notes:

____

R1 Part 1.3

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.

Registered Entity Response (Required):
Question: Is R1 Part 1.3 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	For a change that deviates from the existing baseline configuration, verify the entity documented one or more processes for updating the baseline configuration as necessary within 30 calendar days of completing the change.
	For each Applicable System, for a change that deviates from the existing baseline configuration, verify the entity updated the baseline configuration as necessary within 30 calendar days of completing the change.

Auditor Notes:

____

R1 Part 1.4

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1 Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2 Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3 Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

Registered Entity Response (Required):
Question: Is R1 Part 1.4 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	For a change that deviates from the existing baseline configuration, verify the entity documented one or more processes to: 1. Determine, prior to the change, required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 2. verify, following the change, that required cyber security controls determined in 1.4.1 are not adversely affected; and 3. document the results of the verification.
	For each change that deviates from the existing baseline configuration, for each Applicable System: 1. Verify that, prior to the change, the entity has determined the required security controls in CIP-005 and CIP-007 that could be impacted by the change; 2. verify that, following the change, the entity has verified that the required cyber security controls determined in 1, above, are not adversely affected; and 3. verify that the entity has documented the results of the verification required by 2, above.

Auditor Notes:

R1 Part 1.5

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

Registered Entity Response (Required):
Question: Is R1 Part 1.5 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R1, Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Where technically feasible, for each change that deviates from the existing baseline configuration verify the entity documented one or more processes that include: 1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 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, for each Applicable System, for each change that deviates from the existing baseline configuration, prior to implementing any change in the production environment: • The entity tested the changes in a test environment; or • the entity tested the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; or • a TFE covers this circumstance.
	Verify that, for each Applicable System, where technically feasible, for each change that deviates from the existing baseline configuration, verify: 1. The entity documented the results of the testing; and 2. if a test environment was used, the entity documented 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.
	If a TFE is applicable to an Applicable System, verify the compensating measures identified by the TFE are in place.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

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

Registered Entity Response (Required):
Question: Is R2 Part 2.1 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the entity documented one or more processes to monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1).
	Verify the entity documented one or more processes to document and investigate detected unauthorized changes.
	For each Applicable System, verify the entity monitored at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1).
	For each Applicable System, verify all detected unauthorized changes were documented and investigated.

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-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

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

R3 Part 3.1

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

Registered Entity Response (Required):
Question: Is R3 Part 3.1 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify the 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 entity conducted a paper or active vulnerability assessment at least once every 15 calendar months.

Auditor Notes:

____

R3 Part 3.2

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

Registered Entity Response (Required):
Question: Is R3 Part 3.2 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Where technically feasible, verify the entity documented one or more processes to, at least once every 36 calendar months: 1. Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 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, was an active vulnerability assessment technically feasible? • If yes, verify: o An active vulnerability assessment was conducted at least once every 36 calendar months, in accordance with 3.2.1; and o results of testing are documented, in accordance with 3.2.2. • If no, verify the TFE's compensating measures are in place.

Auditor Notes:

R3 Part 3.3

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.

Registered Entity Response (Required):
Question: Is R3 Part 3.3 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify the entity documented one or more processes for performing an active vulnerability assessment, prior to adding a new applicable Cyber Asset to a production environment, of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.
	For each Applicable System, was a new applicable Cyber Asset added to a production environment? If yes, verify that an active vulnerability assessment of the new Cyber Asset was performed prior to adding it to a production environment, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.
	If the entity has experienced an exception for CIP Exceptional Circumstances, verify the entity has adhered to any applicable cyber security policies.

Auditor Notes:

R3 Part 3.4

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Registered Entity Response (Required):
Question: Is R3 Part 3.4 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
□ Other: [Provide explanation below]

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-010-2, R3, Part 3.4

This section to be completed by the Compliance Enforcement Authority

	Verify the 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, were any vulnerabilities identified? If yes, 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; and 4. the completion of the action plan, if the planned date of completion has been reached.

Auditor Notes:

____

R4 Supporting Evidence and Documentation

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

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

Registered Entity Response (Required):
Question: Is R4 applicable to this audit? □ Yes □ No
If "No," why not?
□ This entity is not responsible for compliance for any high or medium impact BES Cyber Systems.
□ Other: [Provide explanation below]

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-010-2, R4

This section to be completed by the Compliance Enforcement Authority

Section 1. For Transient Cyber Assets(s) managed by the Responsible Entity:	
	Verify that the Responsible Entity has documented at least one plan for Transient Cyber Asset(s) that includes: 1. Transient Cyber Asset management; 2. Transient Cyber Asset 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 Transient Cyber Asset(s) individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.
	For each individual or group of Transient Cyber Asset(s), verify the 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 Transient Cyber Asset (per Transient Cyber Asset capability): • Security patching, including manual or managed updates; • Live operating system and software executable only from read-only media; • System hardening; or • Other method(s) to mitigate software vulnerabilities. If a Transient Cyber Asset is not fully capable of any of the methods above, then verify the Transient Cyber Asset 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 Transient Cyber Asset capability): • 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 Transient Cyber Asset is not fully capable of any of the methods above, then verify the Transient Cyber Asset 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 Transient Cyber Asset(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 Transient Cyber Asset(s) managed by a party other than the Responsible Entity:	
	Verify that the Responsible Entity has documented at least one plan for Transient Cyber Asset(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 Transient Cyber Asset (per Transient Cyber Asset capability): • Review of installed security patch(es); • Review of security patching process used by the party; • Review of other vulnerability mitigation performed by the party; or • Other method(s) to mitigate software vulnerabilities If a Transient Cyber Asset is not fully capable of any of the methods above, then verify the Transient Cyber Asset 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 Transient Cyber Asset 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 • Other method(s) to mitigate malicious code If a Transient Cyber Asset is not fully capable of any of the methods above, then verify the Transient Cyber Asset 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 Transient Cyber Asset.

Section 3. For Removable Media:	
	Verify that the Responsible Entity has documented at least one plan 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 that the Responsible Entity has implemented the following methods 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: 1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a

	BES Cyber System or Protected Cyber Assets; and 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.

Auditor Notes:

____

Additional Information:

Reliability Standard

The full text of CIP-010-2 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 706
See FERC Order 791

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	06/17/2014	Posted for Public Comment	New Document
DRAFT2v0	09/17/2014	CIP RSAW Development Team	Address comments received in response to DRAFT1v0.
DRAFT3v0	12/10/2014	CIP RSAW Development Team	Address comments received in response to DRAFT2v0.
DRAFT4v0	02/06/2015	CIP RSAW Development Team	Address comments from V5R SDT and address comments in response to DRAFT3v0.
DRAFT4v1	03/10/2015	CIP RSAW Development Team	Address comments from V5R SDT meeting on March 3-4, 2015.