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		
R2	X		X	X	X				X			X	X		
R3	X		X	X	X				X			X	X		
R4	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			
P4.1			
P4.2			
P4.3			
P4.4			
P4.5			
P4.6			
P4.7			

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all EACMS (including all EAP) associated with the BES Cyber System. c. The list of all PACS associated with the BES Cyber System. d. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. Documentation of baseline configuration, identified individually or by group. b. Baseline at a minimum includes Part 1.1.1- 1.1.5. i. Operating system (software and version or firmware) ii. Application software (version) iii. Custom software iv. Logical network accessible ports v. Security patches

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify the documentation includes the baseline configuration, individually or by group. Verify each Baseline at a minimum includes Part 1.1.1- 1.1.5. i. Operating system (software and version or firmware) ii. Application software (version) iii. Custom software (software developed for local entity functions or for a specific task) iv. Logical network accessible ports (TCP 65535 / UDP 65535) v. Security patches (historical and current)
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor: 1. Applicable approved TFEs for this requirement should be retrieved from the Regional Entity's TFE management system.	

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: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES

Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all EACMS (including all EAP) associated with the BES Cyber System. c. The list of all PACS associated with the BES Cyber System. d. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. List of all changes that deviated from existing Part 1.1.1 – 1.1.5 baselines configuration during the audit period. i. Change control ID (or other tracking identifier) ii. Start date iii. Completion Date iv. Brief description of the change v. Unique ID of each Cyber Asset included in the change b. All changes that deviated from existing Part 1.1.1 – 1.1.5 baselines configuration during the audit period were authorized.

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.

	For each device identified in Evidence Set 2 Item 1, verify all changes that deviated from existing Part 1.1.1 – 1.1.5 baselines configuration during the audit period. i. Change control ID (or other tracking identifier) ii. Start date iii. Completion Date iv. Brief description of the change v. Unique ID of each Cyber Asset included in the change
	For each device identified in Evidence Set 2 Item 1, verify each change was authorized by the individual or group with proper authority.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor: 1. It will be necessary to use professional judgment when assessing the list of physical input/output ports required for operations.	

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 4. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES

Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all EACMS (including all EAP) associated with the BES Cyber System. c. The list of all PACS associated with the BES Cyber System. d. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide: a. Documentation the existing Part 1.1.1 – 1.1.5 baselines configuration was updated as necessary within 30 calendar days of completing the change.

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	For each device identified in Sample Set 2 Item 1: 1. Verify date of each change to baseline configuration. 2. Verify date of update to the baseline configuration documentation. 3. Verify baseline configuration was updated as unnecessary within 30 calendar days of completing the change.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all EACMS (including all EAP) associated with the BES Cyber System. c. The list of all PACS associated with the BES Cyber System. d. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. List of all changes that deviated from the existing Part 1.1.1 – 1.1.5 baselines configuration within the audit period b. An impact assessment identified cyber security controls and verified or tested identified cyber security controls and system availability was not adversely affected prior to a change that deviates from the Part 1.1.1 - 1.1.5 existing baseline configuration. c. An impact assessment identified cyber security controls and verified or tested identified cyber security controls and system availability was not adversely affected following a change that deviates from the Part 1.1.1 - 1.1.5 existing baseline configuration. d. The results of the verification of cyber security controls are documented.

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.

	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify an impact assessment identified cyber security controls and verified or tested identified cyber security controls and system availability was not adversely affected prior to a change that deviates from the Part 1.1.1 - 1.1.5 existing baseline configuration.
	For each device identified in Evidence Set 2 Item 1, verify an impact assessment identified cyber security controls and verified or tested identified cyber security controls and system availability was not adversely affected following a change that deviates from the Part 1.1.1 - 1.1.5 existing baseline configuration.
	For each device identified in Evidence Set 2 Item 1, verify results of the verification of cyber security controls are documented.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. Documentation of all changes that deviated from the existing Part 1.1.1 – 1.1.5 baselines configuration within the audit period. b. For all changes that deviated from the existing Part 1.1.1 – 1.1.5 baselines configuration within the audit period, provide the following evidence i. Prior to implementing any change in the production environment a test was performed in a manner that minimized adverse effects on required cyber security controls. ii. Documented results of testing. iii. The test environment or production environment where the test is performed models the baseline configuration. iv. The test environment or production environment where the test is performed minimized adverse effect on required cyber security controls.

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify prior to implementing any change in the production environment a test was performed in a manner that minimized adverse effects on required cyber security controls.
	For each device identified in Evidence Set 2 Item 1, verify results of testing are documented.
	For each device identified in Evidence Set 2 Item 1, verify test environment or production environment where the test is performed models the baseline configuration.
	For each device identified in Evidence Set 2 Item 1, verify test environment or production environment where the test is performed minimizes adverse effect on required cyber security controls.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor: 1. Applicable approved TFEs for this requirement should be retrieved from the Regional Entity's TFE management system.	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R2 – Security Patch Management. [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-007-5 Table R2 – Security Patch Management 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all EACMS (including all EAP) associated with the BES Cyber System. c. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. Changes to the baseline configuration (as described in Requirement R1, Part 1.1) were monitored at least once every 35 calendar days. b. All detected unauthorized changes were documented and investigated.

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify for the period of the audit 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 device identified in Evidence Set 2 Item 1, verify all detected unauthorized changes were

	documented and investigated.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.

Evidence Set 1:

1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide:
    a. The name or other identification of the BES Cyber System,
    b. The name or other identification of the associated asset,
    c. The type of the associated asset, and
    d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence:
    a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System.
    b. The list of all EACMS (including all EAP) associated with the BES Cyber System.
    c. The list of all PACS associated with the BES Cyber System.
    d. The list of all PCA associated with the BES Cyber System.
2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
    a. A paper or active vulnerability assessment was conducted at least once every 15 calendar month.
        i. Date of the Vulnerability Assessment
        ii. Controls for each BES Cyber System
        iii. Method of the assessment (paper or active)
        iv. Raw output of any tools used to perform the assessment
    b. Last two conducted vulnerability assessments

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify the entity conducted a paper or active vulnerability assessment at least once every 15 calendar months.
	For each device identified in Evidence Set 2 Item 1, verify all were included in the 15 calendar paper or a active vulnerability assessment.
	Verify last two conducted vulnerability assessments were completed in order to establish a bookend of the 15 calendar month requirement.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. Evidence an active vulnerability assessment was conducted at least once every 36 calendar month. i. Date of the Vulnerability Assessment ii. Controls for each BES Cyber System iii. Method of the assessment (paper or active) iv. Raw output of any tools used to perform the assessment b. Last two conducted vulnerability assessments c. Test environment or production environment was used in 36 calendar month vulnerability assessment. d. If test environment was used in vulnerability assessment i. Description of test environment ii. How test environment models the baseline configuration of the BES Cyber System in a production environment e. If production environment was used in vulnerability assessment i. How test was performed in a manner that minimized adverse effects f. Results of the vulnerability assessment g. If test environment was used in vulnerability assessment i. Differences between the test environment and the production environment ii. Measures used to account for any differences in operation between the test and production environments.

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**	**Document**	**Relevant**	**Description of Applicability**

		or Version	Date	Page(s) or Section(s)	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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify an active vulnerability assessment was conducted at least once every 36 calendar month and included the following: i. Date of the Vulnerability Assessment ii. Controls for each BES Cyber System iii. Method of the assessment iv. Raw output of any tools used to perform the assessment
	For each device identified in Evidence Set 2 Item 1, verify the last two vulnerability assessments were completed as required in order to establish a bookend of the 36 calendar month requirement.
	For each device identified in Evidence Set 2 Item 1, verify a test environment or production environment was used in 36 calendar month vulnerability assessment. a. If test environment was used in vulnerability assessment i. Verify test environment models the baseline configuration of the BES Cyber System in a production environment. b. If production environment was used in vulnerability assessment i. Verify test was performed in a manner that minimized adverse effects.
	For each device identified in Evidence Set 2 Item 1, verify results of the vulnerability assessment a. If test environment was used in vulnerability assessment i. Verify differences between the test environment and the production environment ii. Verify measures used to account for any differences in operation between the test and production environments
	Verify last two conducted vulnerability assessments were completed in order to establish a bookend of the 15 calendar month requirement.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES

Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all EACMS (including all EAP) associated with the BES Cyber System. c. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. An active vulnerability assessment was conducted prior to adding a new applicable Cyber Asset to a production environment. i. Date new Cyber Asset added to production ii. Where there any CIP Exceptional Circumstances within the period of the audit? iii. Method of the assessment iv. Raw output of any tools used to perform the assessment

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify an active vulnerability assessment was conducted prior to adding a new applicable Cyber Asset to a production environment. i. Date new Cyber Asset added to production

	ii. Where there any CIP Exceptional Circumstances within the period of the audit? iii. Method of the assessment iv. Raw output of any tools used to perform the assessment
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence:
   a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System.
   b. The list of all EACMS (including all EAP) associated with the BES Cyber System.
   c. The list of all PACS associated with the BES Cyber System.
   d. The list of all PCA associated with the BES Cyber System.
2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. Results of the assessment conducted according to Parts 3.1, 3.2, and 3.3.
      i. Action plan to remediate or mitigate vulnerabilities identified in the assessments
      ii. Planned date of completing the action plan
      iii. Execution status of any radiation or mitigation action items

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

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	From the entity's response to Evidence Set 1, select a sample of BES Cyber Systems. Provide this sample set to the entity for use in creating Evidence Set 2.
	For each device identified in Evidence Set 2 Item 1, verify results of the assessment conducted according to Parts 3.1, 3.2, and 3.3. i. Action plan to remediate or mitigate vulnerabilities identified in the assessments ii. Planned date of completing the action plan iii. Execution status of any radiation or mitigation action items

	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. 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 R4 – Transient Cyber Asset & Removable Media Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R4 Part 4.1

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

Registered Entity Response (Required):
Question: Is R4 Part 4.1 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. Documentation of any CIP Exceptional Circumstances within the period of the audit. b. Date of any Transient Cyber Asset usage within the period of the audit c. Documented authorization of Transient Cyber Asset prior to usage including: i. Users, individually or by group/role. ii. Locations, individually or by group/role. iii. Defined acceptable use. iv. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).

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, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	Verify if the entity had CIP Exceptional Circumstances within the period of the audit.
	Verify if the entity used Transient Cyber Asset within the period of the audit and date of use.
	Verify the entity authorized the usage of Transient Cyber Assets prior to initial use.
	Ensure authorization included: i. Users, individually or by group/role. ii. Locations, individually or by group/role. iii. Defined acceptable use. iv. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R4 Part 4.2

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).

Registered Entity Response (Required):
Question: Is R4 Part 4.2 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement

Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence:

a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System.
b. The list of all PCA associated with the BES Cyber System.

2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. Method(s) used to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).

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, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has one or more methods documented and deployed to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R4 Part 4.3

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).

Registered Entity Response (Required):
Question: Is R4 Part 4.3 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set,

provide the following evidence:

a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System.
b. The list of all PCA associated with the BES Cyber System.

2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. Date(s) Removable Media used on applicable systems within the period of the audit.
   b. Method(s) used to detect malicious code on Removable Media prior to use on applicable systems.

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, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the date(s) Removable Media used on applicable systems within the period of the audit.
	Verify the entity used method(s) to detect malicious code on Removable Media prior to use on applicable systems.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R4 Part 4.4

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

Registered Entity Response (Required):
Question: Is R4 Part 4.4 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence:
   a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System.
   b. The list of all PCA associated with the BES Cyber System.
2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. Threat of detected malicious code for Transient Cyber Assets was mitigated.
   b. Threat of detected malicious code for Removable Media was mitigated.

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, Part 4.4

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify threat of detected malicious code for Transient Cyber Assets was mitigated.
	Verify threat of detected malicious code for Removable Media was mitigated.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R4 Part 4.5

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Registered Entity Response (Required):
Question: Is R4 Part 4.5 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement

Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence:

a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System.
b. The list of all PCA associated with the BES Cyber System.

2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. Signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns were updated.

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, Part 4.5

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns were updated.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R4 Part 4.6

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets prior to use for modifications that deviate from authorization per Part 4.1.4. Take one of the following actions prior to use for modification(s) identified: • Remediate by returning the Transient Cyber Asset to the authorized state in Part 4.1.4; or • Update the authorized state in Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.

Registered Entity Response (Required):
Question: Is R4 Part 4.6 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES

Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence: a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System. b. The list of all PCA associated with the BES Cyber System. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. Transient Cyber Assets were evaluated prior to use for modifications that deviate from authorization per Part 4.1.4. b. One of the following actions were taken prior to use for modification(s) identified: i. Transient Cyber Asset was returned to the authorized state in Part 4.1.4 and remediated; or ii. The authorized state in Part 4.1.4 was updated.

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, Part 4.6

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify Transient Cyber Assets were evaluated prior to use for modifications that deviate from authorization per Part 4.1.4.
	Verify one of the following actions were taken prior to use for modification(s) identified: i. Verify Transient Cyber Asset were returned to the authorized state in Part 4.1.4 and remediated; or ii. Verify the authorized state in Part 4.1.4 was updated.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R4 Part 4.7

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	At least once every 35 calendar days, or prior to use, evaluate Transient Cyber Assets to ensure security patches are up-to-date. Take one of the following actions prior to use: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

Registered Entity Response (Required):
Question: Is R4 Part 4.7 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, and

d. The impact rating of the BES Cyber System.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of BES Cyber Systems provided in response to Sample Set 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the following evidence:
   a. The list of all BES Cyber Assets and Cyber Assets which comprise the BES Cyber System.
   b. The list of all PCA associated with the BES Cyber System.
2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. Transient Cyber Assets were evaluated to ensure security patches are up-to-date, at least once every 35 calendar days or prior to use.
   b. One of the following actions were taken prior to use:
      i. Applied the applicable patches;
      ii. Created a dated mitigation plan; or
      iii. Revised an existing mitigation plan.
   c. Mitigation plans included the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.

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, Part 4.7

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify Transient Cyber Assets were evaluated to ensure security patches are up-to-date, at least once

	every 35 calendar days or prior to use.
	Verify one of the following actions were taken prior to use: i. The entity applied the applicable patches; ii. The entity created a dated mitigation plan; or iii. The entity revised an existing mitigation plan.
	Verify mitigation plans included the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

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

Selected Glossary Terms

Term	Acronym	Definition
BES Cyber Asset		A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System		One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
CIP Exceptional Circumstances		A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.
CIP Senior Manager		A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.
Control Center		One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in realtime to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
Cyber Assets		Programmable electronic devices, including the hardware, software, and data in those devices.
Cyber Security Incident		A malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.
Electronic Access Control or Monitoring Systems	EACMS	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.
Electronic Access Point	EAP	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
Electronic Security Perimeter	ESP	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
External Routable Connectivity		The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
Physical Access Control Systems	PACS	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security	PSP	The physical border surrounding locations in which BES Cyber Assets,

Perimeter		BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Assets	PCA	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1v0	06/17/2014	Posted for Industry Comment	New Document

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.