



Reliability Standard Audit Worksheet¹

CIP-003-9 – Cyber Security — Security Management Controls

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	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		

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 RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity’s adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which 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.

Attachment 1

R4	X	*	X	X		X		X	X		
----	---	---	---	---	--	---	--	---	---	--	--

* CIP-003-9 is only applicable to DPs that own certain UFLS, UVLS, RAS, Protection Systems, or Cranking Paths. See CIP-003-9 Section 4, Applicability, for details.

Legend:

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

Findings

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

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

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Attachment 1

Subject Matter Experts

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

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

SME Name	Title	Organization	Requirement(s)

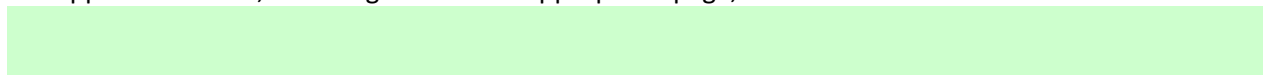
R1 Supporting Evidence and Documentation

- R1.** Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- 1.1.** For its high impact and medium impact BES Cyber Systems, if any:
 - 1.1.1.** Personnel and training (CIP-004);
 - 1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
 - 1.1.3.** Physical security of BES Cyber Systems (CIP-006);
 - 1.1.4.** System security management (CIP-007);
 - 1.1.5.** Incident reporting and response planning (CIP-008);
 - 1.1.6.** Recovery plans for BES Cyber Systems (CIP-009);
 - 1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
 - 1.1.8.** Information protection (CIP-011); and
 - 1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
 - 1.2.** For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
 - 1.2.1.** Cyber security awareness;
 - 1.2.2.** Physical security controls;
 - 1.2.3.** Electronic access controls;
 - 1.2.4.** Cyber Security Incident response;
 - 1.2.5.** Transient Cyber Assets and Removable Media malicious code risk mitigation; and
 - 1.2.6.** Vendor electronic remote access security controls; and
 - 1.2.7.** Declaring and responding to CIP Exceptional Circumstances.
- M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

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-003-9, R1

This section to be completed by the Compliance Enforcement Authority

	<p>For its high impact and medium impact BES Cyber Systems, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics:</p> <ol style="list-style-type: none"> 1. Personnel and training (CIP-004); 2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 3. Physical security of BES Cyber Systems (CIP-006); 4. System security management (CIP-007); 5. Incident reporting and response planning (CIP-008); 6. Recovery plans for BES Cyber Systems (CIP-009); 7. Configuration change management and vulnerability assessments (CIP-010); 8. Information protection (CIP-011); and 9. Declaring and responding to CIP Exceptional Circumstances.
	<p>For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics:</p> <ol style="list-style-type: none"> 1. Cyber security awareness; 2. Physical security controls; 3. Electronic access controls; 4. Cyber Security Incident response 5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and 6. Vendor electronic remote access security controls; and 7. Declaring and responding to CIP Exceptional Circumstances.
	<p>Verify each policy used to meet this Requirement has been reviewed at least once every 15 calendar months.</p>
	<p>Verify the CIP Senior Manager has approved each policy used to meet this Requirement at least once every 15 calendar months.</p>
	<p>Verify the Responsible Entity has achieved the security objective of instituting cyber security policies that will preserve the availability, integrity, and confidentiality of systems that support the reliable operation of the BES.</p>
<p>Note to Auditor: Per Attachment 1, “Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.”</p>	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

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-003-9, R2

This section to be completed by the Compliance Enforcement Authority

	<p><u>Attachment 1, Section 1</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.</p>
	<p><u>Attachment 1, Section 1</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented its plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.</p>
	<p><u>Attachment 1, Section 1</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of ensuring personnel with access to low impact BES Cyber Systems remain aware of cyber security practices.</p>
	<p><u>Attachment 1, Section 2</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to control physical access, based on need as determined by the Responsible Entity, to:</p> <ol style="list-style-type: none"> 1. The asset or the locations of the low impact BES Cyber Systems within the asset; and 2. The Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
	<p><u>Attachment 1, Section 2</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented its plan to control physical access.</p>
	<p><u>Attachment 1, Section 2</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of controlling physical access to:</p> <ol style="list-style-type: none"> 1. The asset or the locations of the low impact BES Cyber Systems within the asset; and 2. The Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
	<p><u>Attachment 1, Section 3.1</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to control inbound and outbound electronic access, based on need as determined by the Responsible Entity, for any communications that are:</p> <ol style="list-style-type: none"> 1. Between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); 2. Using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and 3. Not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).
	<p><u>Attachment 1, Section 3.1</u></p>

Attachment 1

	For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented its plan to control electronic access.
	<u>Attachment 1, Section 3.1</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of permitting only necessary inbound and outbound access to its low impact BES Cyber Systems.
	<u>Attachment 1, Section 3.2</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.
	<u>Attachment 1, Section 3.2</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented the plan to authenticate Dial-up Connectivity.
	<u>Attachment 1, Section 3.2</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of authenticating all Dial-up Connectivity, per Cyber Asset capability, where such connectivity permits access to its low impact BES Cyber Systems.
	<u>Attachment 1, Section 4</u> For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented one or more Cyber Security Incident response plan(s) that include: <ol style="list-style-type: none"> 1. Identification, classification, and response to Cyber Security Incidents; 2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law; 3. Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals; 4. Incident handling for Cyber Security Incidents; 5. Testing each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and 6. Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	<u>Attachment 1, Section 4</u> For each asset containing a low impact BES Cyber System, if the Responsible Entity responded to a Cyber Security Incident, verify the Responsible Entity implemented the Cyber Security Incident response plan.
	<u>Attachment 1, Section 4.5</u> Verify the Responsible Entity tested each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or

Attachment 1

	(3) using an operational exercise of a Reportable Cyber Security Incident.
	<u>Attachment 1, Section 4.6</u> Verify the Responsible Entity updated each Cyber Security Incident response plan, if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	<u>Attachment 1, Section 4</u> Verify the Responsible Entity is prepared to achieve the security objective of minimizing the adverse impact to the BES of a possible Cyber Security Incident affecting low impact BES Cyber Systems.
	<u>Attachment 1, Section 5.1, 5.2, 5.2.1</u> Verify the Responsible Entity has documented one or more plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets.
	<u>Attachment 1, Section 5.1, 5.2, 5.2.1</u> Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets.
	<u>Attachment 1, Section 5.1, 5.2, 5.2.1</u> Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets.
	<u>Attachment 1, Section 5.2.2</u> For any method used pursuant to 5.2.1, verify the Responsible Entity has determined whether any additional mitigation actions are necessary and has implemented such actions prior to connecting the Transient Cyber Asset.
	<u>Attachment 1, Section 5.3.1</u> Verify the Responsible Entity has documented one or more plans to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System.
	<u>Attachment 1, Section 5.3.2</u> Verify the Responsible Entity has documented one or more plans to mitigate the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.
	<u>Attachment 1, Section 5.3</u> Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Removable Media.
	<u>Attachment 1, Section 5.3</u> Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Removable Media.
	<u>Attachment 1, Section 6.0</u> For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, verify that the Responsible Entity has documented a

Attachment 1

	process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.
	<u>Attachment 1, Section 6.0</u> For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, verify that the Responsible Entity has implemented a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.
	<u>Attachment 1, Section 6.0</u> For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, verify that the Responsible Entity has mitigated the risk associated with vendor electronic remote access, where such access has been established under Section 3.1.
	<u>Attachment 1, Section 6.1</u> Verify that the process documented and implemented by the Responsible Entity pursuant to section 6.0, includes one or more method(s) for determining vendor electronic remote access.
	<u>Attachment 1, Section 6.2</u> Verify that the process documented and implemented by the Responsible Entity pursuant to section 6.0, includes one or more method(s) for disabling vendor electronic remote access.
	<u>Attachment 1, Section 6.3</u> Verify that the process documented and implemented by the Responsible Entity pursuant to section 6.0, includes one or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.
Note to Auditor: <u>Attachment 1, Section 3</u> <ol style="list-style-type: none">1. For each asset identified as containing a low impact BES Cyber System(s) per CIP-002, the list of assets should identify those assets that have routable protocol communications between low impact BES Cyber System(s) and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions.<ol style="list-style-type: none">a. For these identified assets, obtain as evidence the devices used to control electronic access and the low impact BES Cyber Systems for which they control access.2. For each asset identified as containing a low impact BES Cyber System(s) per CIP-002, the Responsible Entity has an obligation to determine the necessary inbound and outbound routable protocol communications between low impact BES Cyber System(s) and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions. The Responsible Entity must be able to provide a technically sound explanation as to how its electronic access permissions and controls are consistent with the security objective of permitting only necessary inbound and outbound access to low impact BES Cyber Systems.	

Attachment 1

3. The audit team should assess the effectiveness of the Responsible Entity's electronic access control plan as well as the Responsible Entity's adherence to its electronic access control plan.
4. For the inbound and outbound communications that the Responsible Entity has determined to be necessary, the Responsible Entity must identify the electronic access controls used to effectively control access to and from the low impact BES Cyber System(s).
5. The ten reference models included in the Guidelines and Technical Basis section of the Standard provide examples that Responsible Entities may reference for their electronic access controls. Reference models 9 and 10 outline approaches for segmenting network traffic such that there is no routable protocol communications to the low impact BES Cyber System(s).
 - a. Model 9 uses layer-2 network segmentation (VLANs) to control access. The configuration of the devices used to accomplish this must be documented by the Responsible Entity and assessed for its effectiveness in meeting the standard's objective of controlling access to the low impact BES Cyber System(s).
 - b. In Model 10, a single device receives both serial traffic destined for low impact BES Cyber System(s) and routable traffic destined for non-BES Cyber Asset(s). The device, as depicted in the model, logically isolates the serial traffic from the routable traffic. The configurations for the device must be documented by the Responsible Entity and assessed to determine whether or not the electronic access controls effectively meet the objective of controlling access to the low impact BES Cyber System(s).

Attachment 1, Section 5

1. The means of verifying the mitigation of the introduction of malicious code to a low impact BES Cyber System differs depending on whether a Transient Cyber Asset is managed by the Responsible Entity in an ongoing or an on-demand manner. The verification for a Transient Cyber Asset managed in an ongoing manner focuses on the process of preventing malware from being introduced to the Transient Cyber Asset. The verification for a Transient Cyber Asset managed in an on-demand manner focuses on the process used to ensure the Transient Cyber Asset may be safely used in a low impact BES Cyber System environment prior to such use. If the Transient Cyber Asset is managed in both an ongoing and an on-demand manner, then both verification techniques should be employed.

Auditor Notes:

R3 Supporting Evidence and Documentation

- R3.** Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- M3.** An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

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-003-9, R3

This section to be completed by the Compliance Enforcement Authority

	Verify the CIP Senior Manager has been identified by name.
	Verify that any changes made to the CIP Senior Manager were dated and documented within 30 calendar days of the change.
	Verify the CIP Senior Manager is 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.

Auditor Notes:

Attachment 1

R4 Supporting Evidence and Documentation

- R4.** The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- M4.** An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-003-9, R4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented a process to delegate authority, unless no delegations are used.
	Verify that all delegates have been identified by name or title.
	Verify that the delegation of authority includes the specific action delegated.
	Verify specific actions delegated by the CIP Senior Manager are allowed by the CIP

Attachment 1

	Standards.
	Verify that the dates for all delegations have been recorded.
	Verify that the CIP Senior Manager approved all delegations.
	Verify that any changes made to delegations were dated and documented within 30 days of the change.
Note to Auditor: Delegations of the CIP Senior Manager's authority are permitted for the required approvals in CIP-002-5.1, Requirement R2, CIP-007-6, Requirement R2, Part 2.4, and CIP-013-1 R3.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-003-9 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Standards”, “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

See FERC Order 822

See FERC Order 843

See FERC Letter Order in Docket RD19-5-000 Dated July 31, 2019

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Removable Media

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
 - BES Cyber Asset,
 - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
 - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
 - BES Cyber Asset,
 - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
 - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

- Section 1.** Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).
- Section 2.** Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
- Section 3.** Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:
- 3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
 - i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
 - ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
 - iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).
 - 3.2** Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.
- Section 4.** Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:
- 4.1** Identification, classification, and response to Cyber Security Incidents;

- 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;
- 4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- 4.4 Incident handling for Cyber Security Incidents;
- 4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and
- 4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

- 5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (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.
- 5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:
 - 5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (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 the introduction of malicious code.

Attachment 1

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

- Section 1.** Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:
- Direct communications (for example, e-mails, memos, or computer-based training);
 - Indirect communications (for example, posters, intranet, or brochures); or
 - Management support and reinforcement (for example, presentations or meetings).
- Section 2.** Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:
- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
 - a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
 - b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.
- Section 3.** Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:
1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
 2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

NERC Reliability Standard Audit Worksheet

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented

NERC Reliability Standard Audit Worksheet

prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
 - steps to preauthorize access;
 - alerts generated by vendor log on;
 - session monitoring;
 - security information management logging alerts;
 - time-of-need session initiation;
 - session recording;
 - system logs; or
 - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
 - disabling vendor electronic remote access user or system accounts;
 - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
 - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
 - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
 - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
 - other operational, procedural, or technical controls.
3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
 - Anti-malware technologies (e.g., full packet inspection technologies);
 - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
 - Automated or manual log reviews;
 - alerting; or
 - other operational, procedural, or technical controls.

NERC Reliability Standard Audit Worksheet

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	9/9/2019	CCTF	New document based on CIP-003-7 RSAW