NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-007-6 — Cyber Security – System Security Management

This section to be completed by the Compliance Enforcement Authority.

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

Applicability of Requirements

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		
R3	X	X	X	X	X				X			X	X		
R4	X	X	X	X	X				X			X	X		
R5	X	X	X	X	X				X			X	X		

Legend:

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

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

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

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

Findings

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

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
P1.1			
P1.2			
R2			
P2.1			
P2.2			
P2.3			
P2.4			
R3			
P3.1			
P3.2			
P3.3			
R4			
P4.1			
P4.2			
P4.3			
P4.4			
R5			
P5.1			
P5.2			
P5.3			
P5.4			
P5.5			
P5.6			
P5.7			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

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 implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-007-6 Table R1– Ports and Services			
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 with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

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 Evidence Set 1 Item 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. Identification of the enabled logical ports which are network accessible. Include, if applicable, documentation of the configuration of host firewalls or other methods of restricting network access to a listening port. For Electronic Access Points, this information is only required for the device's management ports. b. If dynamic ports are in use, provide the following: i. The name of each service that requires dynamic ports. ii. The port range used by each service. iii. The method used to associate service with the dynamic port (e.g., netstat, etc.). c. Documentation of the need (e.g., operational purpose) for all enabled logical network accessible ports. For Electronic Access Points, this information is only required for the device's management ports. d. The comparison of the list of ports actually network accessible to the list of ports needed.

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-007-6, 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.
	For each device identified in Evidence Set 2 Item 1, verify the documentation includes the need for each enabled logical network accessible port on the device. Where a port range is required, verify the associated service is also identified. Verify that the list of needed logical network accessible ports and services does not contain unjustified ports or services. If a logical network accessible port is deemed needed by the inability to disable the port, verify the documentation of the inability to disable the port.
	For each device identified in Evidence Set 2 Item 1, review the list of logical network accessible ports on the device. Where a logical network accessible port is part of a port range, verify the associated service to which the port is bound is also identified.
	In the case where a port is not needed but cannot be disabled, verify that the device is covered by an approved Technical Feasibility Exception.
	For each device identified in Evidence Set 2 Item 1, review the comparison of the needed ports and services with the listening ports and services. Verify that this comparison is complete and correct.
	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-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

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 Evidence Set 1 Item 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. c. The list of all nonprogrammable communication components associated with the BES Cyber System and located inside both a PSP and an ESP. 2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence: a. List of all physical input/output ports (capable of network connectivity, console commands, or Removable Media). b. List of all physical input/output ports (capable of network connectivity, console commands, or Removable Media) that are required for operations, and the basis for that requirement. c. Documentation of the protections provided to physical input/output ports (capable of network connectivity, console commands, or Removable Media) that are not required for operations.

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-007-6, 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.
	For each device identified in Evidence Set 2 Item 1, verify the list of physical input/output ports is complete and correct. This evaluation may be supplemented by physical examination during a site visit.
	For each device identified in Evidence Set 2 Item 1, verify the list of physical input/output ports required

	for operations appears correct.
	For each device identified in Evidence Set 2 Item 1, verify that the unnecessary physical input/output ports are protected against use.
	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.
2. Protections provided to unnecessary physical input/output ports may include, but are not limited to:
    a. Logically disabling the port via operating system or other configuration. If this method is used, the auditor should additionally verify that the port is disabled at the time of the audit. This will address the issue of the port being unintentionally re-enabled by patches or other changes.
    b. Physically disabling the port by unplugging the internal port connector from its source, installing a port lock, or other means.
    c. Physically marking the port such that personnel with physical access to the device are reminded that the port is not to be used. Use of this method on a device that is accessible by personnel other than system administrators may require a Recommendation that the entity improve the physical protections for the device.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 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-007-6 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-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

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 Evidence Set 1 Item 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. Identification of:
        i. The operating system; or
        ii. The firmware where no independent operating system exists;
    b. Identification of any commercially available software installed on the device;
    c. Identification of any open-source application software installed on the device; and
    d. Identification of any custom software installed on the device.
3. For each device identified in response to Evidence Set 2 Item 1 above, provide evidence that the list of software identified in response to Evidence Set 2 Item 2 above is complete.
4. For each item in the the list of software identified in response to Evidence Set 2 Item 2 above, provide:
    a. Name or other identification of the software installed;
    b. Version, release number, and/or revision date of the software installed;
    c. Identification of the source being tracked for cyber security patches, or documentation that no patch source exists.

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-007-6, 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.
	Verify the documented process(es) include provisions for tracking, evaluating, and installing cyber security patches.
	Verify the tracking portion of the documented process(es) includes the identification of one or more sources for cyber security patches.
	For each device identified in Evidence Set 2 Item 1: 1. Verify the documentation of each item of software. 2. Verify the entity has chosen an applicable cyber security patch source. 3. Verify the completeness of the software list.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Part 2.2

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

Registered Entity Response (Required):
Question: Is R2 Part 2.2 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the list of all applicable cyber security patch sources. 2. For each patch source identified in response to Evidence Set 2 Item 1 above, provide the following: a. Identification of each security patch released by each patch source during the audit period, including the date of release; b. Evidence of the evaluation of each security patch for applicability, including: i. Date of evaluation; ii. Results of the evaluation (i.e., applicable or not applicable); and iii. If not applicable, the reason the patch is not applicable.

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-007-5, R2, Part 2.2

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.
	For each patch source identified in Evidence Set 2 Item 1: 1. Verify that security patches from the patch source have been evaluated for applicability at least once every 35 calendar days during the audit period. 2. Verify the results of the evaluations.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Part 2.3

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • 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 and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

Registered Entity Response (Required):
Question: Is R2 Part 2.3 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the list of all applicable cyber security patch sources.
2. For each patch source identified in response to Evidence Set 2 Item 1 above, provide the following:
   a. Identification of each security patch released by each patch source during the audit period which was evaluated as applicable per Part 2.2;
   b. The date of completion of the evaluation of each applicable patch; and
   c. A list of the devices comprising or associated with the BES Cyber System for which each patch is applicable;
3. For each patch identified in response to Evidence Set 2 Item 2 above, provide evidence of the action taken regarding the patch:
   a. For each device to which the patch was applied provide:
      i. Evidence of the application of the patch; and
      ii. Evidence of the date the patch was applied.
   b. If the patch was not applied to all devices comprising or associated with the BES Cyber System for which the patch is applicable, provide:
      i. The associated mitigation plan; and
      ii. The implementation status of the mitigation plan.

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-007-6, R2, Part 2.3

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 applicable security patch, verify that one of the following actions was taken within 35 calendar days of the completion of the evaluation for applicability: • The patch was applied to all devices for which it is applicable; or • A mitigation plan was created; or • A mitigation plan was revised.
	In the case where a mitigation plan was created or revised: 1. Verify the mitigation plan addresses each vulnerability addressed by the security patch; 2. Verify the mitigation plan is sufficient to mitigate each vulnerability addressed by the security patch; 3. Verify the mitigation plan includes a timeframe for completion; 4. Review the timeframe specified by the mitigation plan to determine if it results in mitigation of each vulnerability within a reasonable period; and 5. If the mitigation plan is complete, verify the mitigation plan was completed within the timeframe specified by the mitigation plan, or within the approved extension period per Part 2.4.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
	If mitigation plans are not implemented in a timely manner, based on the needs of the equipment being protected, then an Area of Concern or a Recommendation should be documented.

Note to Auditor:

1. Results-based Requirement: The end result of this Requirement must be the mitigation of vulnerabilities addressed by applicable security patches. The entity has been granted wide latitude by the language of the Requirement regarding how this result is accomplished. It is the function of the auditor to verify that the end result is sufficient to protect the BES.
2. Implementation Timelines: Due to the large variety of circumstances to which this Requirement may apply, there is no specific requirement regarding the time to implement a mitigation plan. The auditor must use professional judgment to accept or express concern over the time frame to implement mitigation plans. While a finding of Possible Violation for an excessively lengthy mitigation timeline is not supported by the language of the Requirement, a documented Area of Concern or Recommendation will ensure that the matter is addressed during risk assessment.

Auditor Notes:

R2 Part 2.4

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	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 each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Registered Entity Response (Required):
Question: Is R2 Part 2.4 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the list of all applicable mitigation plans per CIP-007-6 R2 Part 2.3 which were active at any time during the audit period.
2. For each mitigation plan identified in response to Evidence Set 2 Item 1 above, provide the following:
    a. The mitigation plan;
    b. The status of the mitigation plan (i.e., completed or active);
    c. For completed mitigation plans:
        i. Evidence of the work performed to complete the mitigation plan;
        ii. Evidence of the completion date of the mitigation plan.
    d. For active mitigation plans:
        i. Evidence of the status of the mitigation plan;
        ii. The expected completion date of the mitigation plan.

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-007-5, 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.
	For each completed mitigation plan: 1. Verify the mitigation plan was completed by implementing all provisions of the mitigation plan; 2. Verify the mitigation plan was completed within the specified timeframe. 3. If a revision or an extension was made to a mitigation plan, verify the revision or extension was approved by the CIP Senior manager or delegate.
	For each active mitigation plan: 1. Verify the mitigation plan has not exceeded its implementation timeframe, or its approved

	extension, if any. 2. If a revision or an extension was made to a mitigation plan, verify the revision or extension was approved by the CIP Senior manager or delegate.
	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-007-6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*.

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R3 Part 3.1

CIP-007-6 Table R3 – Malicious Code Prevention			
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	Deploy method(s) to deter, detect, or prevent malicious code.	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, system hardening, policies, etc.).

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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, and its associated EACMS, PACS, and PCA, provide evidence of the deployment of method(s) to deter, detect, or prevent malicious code.

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-007-6, 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.
	For each BES Cyber System identified in Evidence Set 2: 1. Verify that each device comprising the BES Cyber System has one or more methods documented and deployed to deter, detect, or prevent malicious code. 2. Verify that each EACMS, PACS, and PCA associated with the BES Cyber System has one or more methods documented and deployed to deter, detect, or prevent malicious code.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

1. System Approach: The intent of the requirement is that the BES Cyber System as a whole has malware prevention deployed. Each individual component is not required to have the same protection. Not all components will be vulnerable to malware. Of those that are, differing protections may be appropriate for each type of device. For example, a firmware-based device may not be vulnerable to malware if its USB port is protected, such that only authorized personnel may update the firmware. This protection could be considered sufficient to deter the introduction of malicious code.

Auditor Notes:

R3 Part 3.2

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	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	Mitigate the threat of detected malicious code.	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 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.
Processes or methods used to detect malicious code.
List of all instances of detected malicious code, including: • Type of malicious code detected; • Date the malicious code was detected; • Devices affected by the malicious code, if any; • Method of detection; • Mitigation actions taken; • Date the mitigation actions were taken; and

- If the threat of the detected malicious code has not been fully mitigated, the action plan, including timetable, to complete the mitigation.

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-007-6, 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.
	Verify the entity uses one or more methods to detect malicious code.
	For each instance of detected malicious code reviewed, verify the mitigating steps taken are consistent with the process and mitigate the threat of the malicious code.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.

Note to Auditor:

1. Results-based Requirement: The Requirement assumes malicious code will be detected – the entity is therefore required to do so, but the approaches used to perform this detection are not specified.

Auditor Notes:

R3 Part 3.3

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the 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 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.
List of all methods used to deter, detect, or prevent malicious code which use signatures or patterns.
For each method used to deter, detect, or prevent malicious code which uses signatures or patterns, provide the process used to update the signatures or patterns.
For each method used to deter, detect, or prevent malicious code which uses signatures or patterns, provide evidence of the implementation of each process.

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-007-6, 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.
	Verify the processes address testing and installing updates to signatures or patterns.
	Verify the processes are implemented.
	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-007-6 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

R4 Part 4.1

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	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	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

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 Evidence Set 1 Item 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. e. Indication of whether logging is performed at the BES Cyber System level or the Cyber Asset level. 2. If logging is performed at the BES Cyber System level: a. Provide evidence of the types of logging events enabled for the BES Cyber System; b. Provide evidence of the types of logging events enabled for any associated EACMS, including EAP. c. Provide evidence of the types of logging events enabled for any associated PACS. d. Provide evidence of the types of logging events enabled for any associated PCA. e. If any component of the BES Cyber System or any associated device is not capable of logging at least the required event types, provide evidence of the lack of capability. f. Provide evidence that logs for the BES Cyber System are being generated. g. Provide evidence that logs for any associated EACMS are being generated. h. Provide evidence that logs for any associated PACS are being generated. i. Provide evidence that logs for any associated PCA are being generated. 3. If logging is performed at the Cyber Asset level: a. Provide evidence of the types of logging events enabled for each Cyber Asset comprising the BES Cyber System; b. Provide evidence of the types of logging events enabled for any associated EACMS, including EAP. c. Provide evidence of the types of logging events enabled for any associated PACS. d. Provide evidence of the types of logging events enabled for any associated PCA. e. If any Cyber Asset comprising the BES Cyber System or any associated device is not capable of logging at least the required event types, provide evidence of the lack of capability.

f. Provide evidence that logs for each Cyber Asset comprising the BES Cyber System are being generated.
g. Provide evidence that logs for any associated EACMS are being generated.
h. Provide evidence that logs for any associated PACS are being generated.
i. Provide evidence that logs for any associated PCA are being generated.

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-007-6, 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.
	If logging is performed at the BES Cyber System level, for each sampled BES Cyber System and associated EACMS, PACS and PCA: 1. For each of the following event types: successful login attempts, failed access attempts, failed login attempts, and detected malicious code, verify: a. The BES Cyber System or associated device is capable of, and configured for, logging the event type; or b. The BES Cyber System or associated device is not capable of logging the event type. 2. Verify logs are being generated by the BES Cyber System or associated device.
	If logging is performed at the Cyber Asset level, for each Cyber Asset comprising the sampled BES Cyber System and associated EACMS, PACS and PCA: 1. For each of the following event types: successful login attempts, failed access attempts, failed login attempts, and detected malicious code, verify: a. The Cyber Asset or associated device is capable of, and configured for, logging the event type; or b. The Cyber Asset or associated device is not capable of logging the event type. 2. Verify logs are being generated by the Cyber Asset or associated device.

	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-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

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 Evidence Set 1 Item 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 security events determined to necessitate an alert. b. Evidence that such detected security events are configured to generate an alert. c. Evidence that such detected security events generate an alert.

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-007-6, 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 documented one or more processes which address this Part.
	Verify the list of security events determined to necessitate an alert includes: 1. Detected malicious code; 2. Detected failure of logging.
	Verify the security events determined to necessitate an alert are configured to generate an alert.
	Verify alerts are being generated for applicable security events.
	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-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.

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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide evidence that logs pertaining to the BES Cyber System and its associated EACMS (including EAP), PACS, and PCA are retained for at least 90 calendar days.

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-007-6, 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 entity has documented one or more processes which address this Part.
	For each sampled BES Cyber System and its associated EACMS, PACS, and PCA, verify logs are retained for at least 90 calendar days unless: 1. An approved TFE covers one or more of the devices. If this applies, verify the TFE's compensating measures are in place, and review the log retention for the devices not covered by the TFE. 2. A documented CIP Exceptional Circumstance exists. If this applies, review the log retention for devices and timeframes not covered by the CIP Exceptional Circumstance.
	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-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

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 and a set of six calendar months during the audit period to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this

sample set, provide:

a. The process or method used to review logged events.
b. For each calendar month selected, provide evidence of the review of logged events at least every 15 calendar days

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-007-6, 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 the entity has documented one or more processes which address this Part.
	Verify the entity reviews a summary or sampling of logged events.
	Verify the entity reviews logged events at least every 15 calendar days.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R5 Part 5.1

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

Registered Entity Response (Required):
Question: Is R5 Part 5.1 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set and the associated EACMS (including EAP), PACS, and PCA, provide the following: a. Evidence of the method(s) used to enforce authentication of interactive access. b. Evidence of the implementation of the method(s) used to enforce authentication of interactive access.

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-007-6, R5, Part 5.1

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 the entity has documented one or more methods to enforce authentication of interactive user access.
	Verify either: 1. The entity has implemented the method(s) to enforce authentication of interactive user access, or 2. An approved TFE is in place. If a TFE is in place, verify the compensating measures have been implemented.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R5 Part 5.2

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	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	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

Registered Entity Response (Required):
Question: Is R5 Part 5.2 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set and associated EACMS (including EAP), PACS, and PCA, provide the following evidence:
   a. The inventory of all known default or generic account types;
   b. Evidence of the status (i.e., enabled or disabled) of each account in the inventory.

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-007-6, R5, Part 5.2

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.
	Verify the entity has identified and inventoried all known or enabled generic accounts.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R5 Part 5.3

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

Registered Entity Response (Required):
Question: Is R5 Part 5.3 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set and the associated EACMS (including EAP), PACS, and PCA, provide the following evidence: a. The list of individuals with authorized access to shared accounts.

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-007-6, R5, Part 5.3

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.
	Verify the entity has identified individuals with authorized access to shared accounts.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R5 Part 5.4

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	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	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

Registered Entity Response (Required):
Question: Is R5 Part 5.4 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set and the associated EACMS (including EAP), PACS, and PCA, provide:
   a. Evidence of change of the known default password(s) for each device;
   b. For Cyber Assets that do not have the ability to change one or more default passwords, provide evidence of the inability to change the passwords.

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-007-6, R5, Part 5.4

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.
	For devices with the ability to change default passwords, verify the entity has changes the default passwords.
	For Cyber Assets that do not have the ability to change default passwords, verify the inability to do so.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R5 Part 5.5

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	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 password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

Registered Entity Response (Required):
Question: Is R5 Part 5.5 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set and the associated EACMS (including EAP), PACS, and PCA, provide:
    a. The method used to enforce the password length requirement (i.e., technical or procedural) for password-only authentication for interactive user access.
        i. If password length is enforced by a technical method, provide evidence of configuration to enforce this requirement.
        ii. If password length is enforced by a procedural method:
            1. Provide the procedure used to enforce this requirement.
            2. Provide evidence (e.g., training content, email notification, etc.) that this procedure is enforced.
    b. The method used to enforce the password complexity requirement (i.e., technical or procedural) for password-only authentication for interactive user access.
        i. If password complexity is enforced by a technical method, provide evidence of configuration to enforce this requirement.
        ii. If password complexity is enforced by a procedural method:
            1. Provide the procedure used to enforce this requirement.
            2. Provide evidence (e.g., training content, email notification, etc.) that this procedure is enforced.

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-007-6, R5, Part 5.5

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.
	For password-only authentication for interactive user access, verify password length is enforced by either technical or procedural methods.
	For password-only authentication for interactive user access, verify password complexity is enforced by either technical or procedural methods.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.

Note to Auditor:

1. This Part does not apply to multi-factor authentication.
2. This part does not apply to read-only access to a Cyber Asset, in which the configuration of the Cyber Asset cannot be changed and there is no way for the Cyber Asset to affect the BES.
3. If a device has the technical capability to enforce password length and/or complexity, then that method should normally be used. If the entity chooses a procedural method of enforcement when a technical method is available, the circumstances regarding this choice should be reviewed, and the auditor should consider documenting a Recommendation to improve enforcement of this Part.

Auditor Notes:

R5 Part 5.6

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

Registered Entity Response (Required):
Question: Is R5 Part 5.6 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set and the associated EACMS (including EAP), PACS, and PCA, provide: a. The method used to enforce the password change requirement (i.e., technical or procedural) for password-only authentication for interactive user access. i. If password change is enforced by a technical method, provide evidence of configuration to enforce this requirement. ii. If password change is enforced by a procedural method: 1. Provide the procedure used to enforce this requirement. 2. Provide evidence (e.g., training content, email notification, etc.) that this procedure is enforced.

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-007-6, R5, Part 5.6

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 the entity has documented one or more processes which address this Part.
	If a password for password-only authentication for interactive user access cannot be changed, verify an approved TFE covers this circumstance, and verify the compensating measures described by the TFE are in place.
	If a password for password-only authentication for interactive user access can be changed, verify password ageing is enforced by either technical or procedural methods.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.

Note to Auditor:

1. This Part does not apply to multi-factor authentication.

2. This part does not apply to read-only access to a Cyber Asset, in which the configuration of the Cyber Asset cannot be changed and there is no way for the Cyber Asset to affect the BES.
3. If a device has the technical capability to enforce password ageing, then that method should normally be used. If the entity chooses a procedural method of enforcement when a technical method is available, the circumstances regarding this choice should be reviewed, and the auditor should consider documenting a Recommendation to improve enforcement of this Part.

Auditor Notes:

R5 Part 5.7

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

Registered Entity Response (Required):
Question: Is R5 Part 5.7 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 Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set and the associated EACMS (including EAP), PACS, and PCA, provide:
   a. The method used to address unsuccessful authentication attempts (i.e., limiting attempts or alerting).
   b. Evidence of the configuration used to enforce this requirement.

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-007-6, R5, Part 5.7

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 the entity has documented one or more processes which address this Part.
	If the number of unsuccessful authentication attempts is limited, verify the evidence of configuration supports this method.
	If alerts are generated after a threshold of unsuccessful authentication attempts, verify the evidence of configuration supports this method.
	If neither method is used, verify an approved TFE covers this circumstance, and verify the compensating measures described by the TFE are in place.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.

Note to Auditor:

1. If the entity sets an unreasonably high threshold for unsuccessful authentication attempts, this fact should be documented in a Recommendation.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-007-6 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

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

BES Cyber Asset (BCA): 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 Transient Cyber Asset is not a BES Cyber Asset.

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 Circumstance: 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 Systems.

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 Perimeter (PSP): The physical border surrounding locations in which BES Cyber Assets, 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 Transient Cyber Asset is not a Protected Cyber Asset.

Removable Media: Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples 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. A Cyber Asset is not Removable Media.

Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets 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 Public 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.