NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-007-7 — 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	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		
R3	X	X	X	X		X			X	X		
R4	X	X	X	X		X			X	X		
R5	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			
R2			
R3			
R4			
R5			

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-007-7 Table R1 – System Hardening*. *[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-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group; • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessable logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed network accessibility.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.
	Verify the Responsible Entity has implemented one or more processes to disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.
	If a system is incapable of disabling or preventing unnedded routable protocol network accessibility on each Applicable System, verify that compensating measures are implemented.

Auditor Notes:

____

R1 Part 1.2

CIP-007-7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.
	For each Cyber Asset of an Applicable System, verify that the unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media are protected against use.

Auditor Notes:

R1 Part 1.3

CIP-007-7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting either: High impact BCS and their associated PCA. Medium impact BCS and their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets

Registered Entity Response (Required):
Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.
	Verify the Responsible Entity has implemented one or more processes that mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.

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-007-7 Table R2 – Cyber 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-007-7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches. 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 Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more patch management processes for tracking, evaluating, and installing cyber security patches for Applicable Systems.
	Verify that the tracking portion of each patch management process includes the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.
	For each Applicable System, verify at least one of the following is true: • The Responsible Entity has identified one or more patching sources; • The Responsible Entity has documented that the Applicable System is not updateable; or • The Responsible Entity has documented that no patching source exists.

Auditor Notes:

R2 Part 2.2

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.2
This section to be completed by the Compliance Enforcement Authority

□	Verify the Responsible Entity has documented one or more processes to evaluate cyber security patches

	for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1, at least once every 35 calendar days.
	For each identified patch source, verify that cyber security patches have been evaluated for applicability at least once every 35 calendar days.
	For each identified patch source, verify the results of the evaluations for applicability.

Auditor Notes:

R2 Part 2.3

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BES Cyber System and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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; • 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 cyber 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 cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of 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 cyber security patch and a timeframe for the completion of these mitigations.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes, for applicable patches identified in Part 2.2, to take one of the following actions within 35 calendar days of the evaluation completion: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan.
	Verify the Responsible Entity has documented one or more processes for its mitigation plans that requires the inclusion of planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.
	For each applicable cyber 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; • A mitigation plan was created; or • A mitigation plan was revised.
	In the case where a mitigation plan was created or revised, verify the mitigation plan includes planned actions to mitigate the vulnerabilities addressed by each cyber security patch, and that the mitigation plan includes a timeframe for completion.
Note to Auditor: Entities may choose to use a single mitigation plan for multiple patches. In this case, the mitigation plan must have planned actions to mitigate the vulnerabilities addressed by each security patch.	

Auditor Notes:

R2 Part 2.4

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that, for each mitigation plan

	created or revised in Part 2.3, require implementation of 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.
	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; and 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.

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-007-7 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-007-7 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-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to deploy method(s) to deter, detect, or prevent malicious code.
	Verify that each Applicable System has one or more documented methods deployed to deter, detect, or prevent malicious code.

Auditor Notes:

R3 Part 3.2

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that mitigate the threat of

	detected malicious code.
	For each instance of detected malicious code, verify the threat of the malicious code was mitigated.
Note to Auditor: It may not be necessary to remove malicious code from a device in order to mitigate the threat of that malicious code. For example, it may be possible to contain malicious code by blocking communication with its command and control servers and by preventing its spread to other systems. Then the malicious code can be removed at a later time such as a plant outage.	

Auditor Notes:

R3 Part 3.3

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

Registered Entity Response (Required):
Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	For those methods identified in Part 3.1 that use signatures or patterns, verify the Responsible Entity

	has documented one or more processes to update the signatures or patterns. The process must address testing and installing the signatures or patterns.
	For each method deployed to deter, detect, or prevent malicious code that uses signatures or patterns, verify the associated process addresses testing and installing updates to signatures or patterns.
	For each method deployed to deter, detect, or prevent malicious code that uses signatures or patterns, verify the associated process is implemented.

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-007-7 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-007-7 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-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at 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; and 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 Applicable 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):
Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 1. Detected successful login attempts; 2. detected failed access attempts and failed login attempts; and 3. detected malicious code.
	For each event type required for identification of or after the fact investigation of Cyber Security Incidents: • If logging of the event type is performed at the BES Cyber System level, for each Applicable System, verify: ○ The BES Cyber System is capable of, and configured for, logging the event type; ○ The BES Cyber System is generating logs of the event type; or ○ The BES Cyber System is not capable of logging the event type. • If logging of the event type is performed at the Cyber Asset level, for each Cyber Asset of an Applicable System, verify: ○ The Cyber Asset is capable of, and configured for, logging the event type; ○ The Cyber Asset is generating logs of the event type; or ○ The Cyber Asset is not capable of logging the event type.

Auditor Notes:

R4 Part 4.2

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to 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 system capability: 1. Detected malicious code from Part 4.1; and 2. detected failure of Part 4.1 event logging.
	Verify the Responsible Entity has determined the security events that necessitate an alert.
	Verify the security events determined to necessitate an alert include, at a minimum: 1. Detected malicious code; and 2. detected failure of logging.
	For each of the security events determined to necessitate an alert: 1. If alerting is performed on a per Cyber Asset basis, is the Cyber Asset capable of alerting on the event type? 1. If yes, verify either: i. Alerting is configured for the Cyber Asset for the event type; or ii. an actual alert has been generated. 2. If no, verify the inability of the Cyber Asset to generate an alert for the event type. 2. If alerting is performed on a per BES Cyber System basis, is the BES Cyber System capable of alerting on the event type? 1. If yes, verify either: i. Alerting is configured for the BES Cyber System for the event type; or ii. an actual alert has been generated. 2. If no, verify the inability of the BES Cyber System to generate an alert for the event type.

Auditor Notes:

R4 Part 4.3

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, 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 calendar days or greater.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to retain applicable security event

	logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.
	For each Applicable System, verify logs are retained for at least 90 consecutive calendar days unless: • The system is incapable of retaining logs; or • A documented CIP Exceptional Circumstance exists.
	If a system is incapable of retaining logs for at least 90 consecutive calendar days, verify that compensating measures are implemented.
	If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R4 Part 4.4

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security 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, findings from the review (if any), and dated documentation showing the review occurred.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.
	Verify the Responsible Entity reviews a summary or sampling of logged security events at least every 15 calendar days to identify otherwise undetected Cyber Security Incidents.

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-007-7 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-007-7 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-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to have a method(s) to enforce authentication of interactive user access, per system capability.
	For each Applicable System, verify the Responsible Entity enforces authentication of interactive user access per system capability
	If a system is incapable of enforcing authentication of interactive user access, verify that compensating measures are implemented.

Auditor Notes:

R5 Part 5.2

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to 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).
	For each Cyber Asset of an Applicable System, verify the Responsible Entity has identified and inventoried all known enabled default or other generic account types. These account types may be identified by system, by groups of systems, by location, or by system type.

Auditor Notes:

R5 Part 5.3

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

Registered Entity Response (Required):
Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to identify individuals who have authorized access to shared accounts.

	For each Cyber Asset of an Applicable System, verify the Responsible Entity has identified individuals with authorized access to shared accounts.
Note to Auditor: The Responsible Entity is permitted flexibility in the way shared accounts may be documented. Shared accounts may be documented by Cyber Asset or BES Cyber System. Additionally, individuals with authorized access to shared accounts may be listed individually or by role.	

Auditor Notes:

R5 Part 5.4

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to change known default passwords, per system capability.

	For Applicable Systems with the capability to change default passwords, verify the Responsible Entity has changed the known default passwords.
	If a system is incapable of changing default passwords, verify that compensating measures are implemented.

Auditor Notes:

R5 Part 5.5

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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 Applicable Systems; 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 Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots 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):
Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.5

This section to be completed by the Compliance Enforcement Authority

	For password-only authentication for interactive user access, verify the Responsible Entity has documented one or more processes to either technically or procedurally enforce the following password parameters: 1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 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 Applicable System.
	For each Applicable System, for password-only authentication for interactive user access, verify password length is enforced by either technical or procedural methods, per 5.5.1.
	For each Applicable System, for password-only authentication for interactive user access, verify password complexity is enforced by either technical or procedural methods, per 5.5.2.
Note to Auditor: This Part does not apply to multi-factor authentication.	

Auditor Notes:

____

R5 Part 5.6

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots 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):
Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.6

This section to be completed by the Compliance Enforcement Authority

	For password-only authentication for interactive user access, verify the Responsible Entity has documented one or more processes to either technically or procedurally enforce password changes or

	an obligation to change the password at least once every 15 calendar months, per system capability.
	For Applicable Systems, if a password for password-only authentication for interactive user access cannot be changed, verify that the system is incapable of changing the password.
	For Applicable Systems, if a password for password-only authentication for interactive user access can be changed, verify a password change, at least every 15 calendar months, is enforced by either technical or procedural methods.
	If a system is incapable of changing a password for password-only authentication for interactive user access, verify that compensating measures are implemented.
Note to Auditor: This Part does not apply to multi-factor authentication.	

Auditor Notes:

R5 Part 5.7

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

Registered Entity Response (Required):
Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.7

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication

	attempts, per system capability.
	If the number of unsuccessful authentication attempts is limited, verify the configuration.
	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 that compensating measures are implemented.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-007-7 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

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

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

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

Sampling Methodology

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

Regulatory Language

See FERC Order 822

Revision History for RSAW

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