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

DRAFT NERC Reliability Standard Audit Worksheet

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.

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

	Verify the entity has documented one or more processes which address this Part.
	For each applicable Cyber Asset that has no provision for disabling or restricting logical ports, verify this circumstance.
	For each applicable Cyber Asset that has provision for disabling or restricting logical ports, for each enabled logical network accessible dynamic port on the Cyber Asset, verify the port range or service has been documented.
	For each applicable Cyber Asset that has provision for disabling or restricting logical ports, for each enabled logical network accessible port on the Cyber Asset, verify one of the following: • The enabled logical network accessible port has a documented need; or • A TFE covers the enabled logical network accessible port.
Note to Auditor:	

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.

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

DRAFT NERC Reliability Standard Audit Worksheet
Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD
RSAW Version: RSAW CIP-007-6 DRAFT2v0   Revision Date: September 17, 2014   RSAW Template: RSAW2014R1.3

6

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

	Verify the entity has documented one or more processes which address this Part.
	For each applicable device, verify that the unnecessary physical input/output ports used for network connectivity, console commands, or removable media are protected against use.
Note to Auditor:	

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.

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

	Verify the entity has documented one or more processes which address this Part.
	Verify each documented process includes a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. 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 Cyber Assets that are updateable and for which a patching source exists.
	For each item of software or firmware installed on the Cyber Asset, verify one of the following is true: • The entity has identified one or more patching sources; or • The entity has documented that the software or firmware is not updateable; or • The entity has documented that no patching source exists.
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.

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 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more processes which address this Part.
	For each identified patch source, verify that security patches from the patch source have been evaluated for applicability at least once every 35 calendar days during the audit period.
	For each identified patch source, verify the results of the evaluations for applicability.
Note to Auditor:	

Auditor Notes:

R2 Part 2.3

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.

CIP-007-6 Table R2 – Security Patch Management

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.

Registered Entity Evidence (Required):

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

File Name	Document Title	Revision	Document	Relevant	Description of Applicability

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

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

Compliance Assessment Approach Specific to CIP-007-6, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	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, verify the mitigation plan mitigates each vulnerability addressed by each security patch, and that the mitigation plan includes a timeframe for completion.
Note to Auditor:	

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.

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 2.4
This section to be completed by the Compliance Enforcement Authority

	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.
Note to Auditor:	

Auditor Notes:

DRAFT NERC Reliability Standard Audit Worksheet
Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD
RSAW Version: RSAW CIP-007-6 DRAFT2v0   Revision Date: September 17, 2014   RSAW Template: RSAW2014R1.3

16

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 R3 Part 3.1 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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

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

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

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

Compliance Assessment Approach Specific to CIP-007-6, R3, Part 3.1
This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more processes which address this Part.
	For each applicable Cyber Asset, verify that each device has one or more methods documented and deployed to deter, detect, or prevent malicious code.

Note to Auditor:

Auditor Notes:
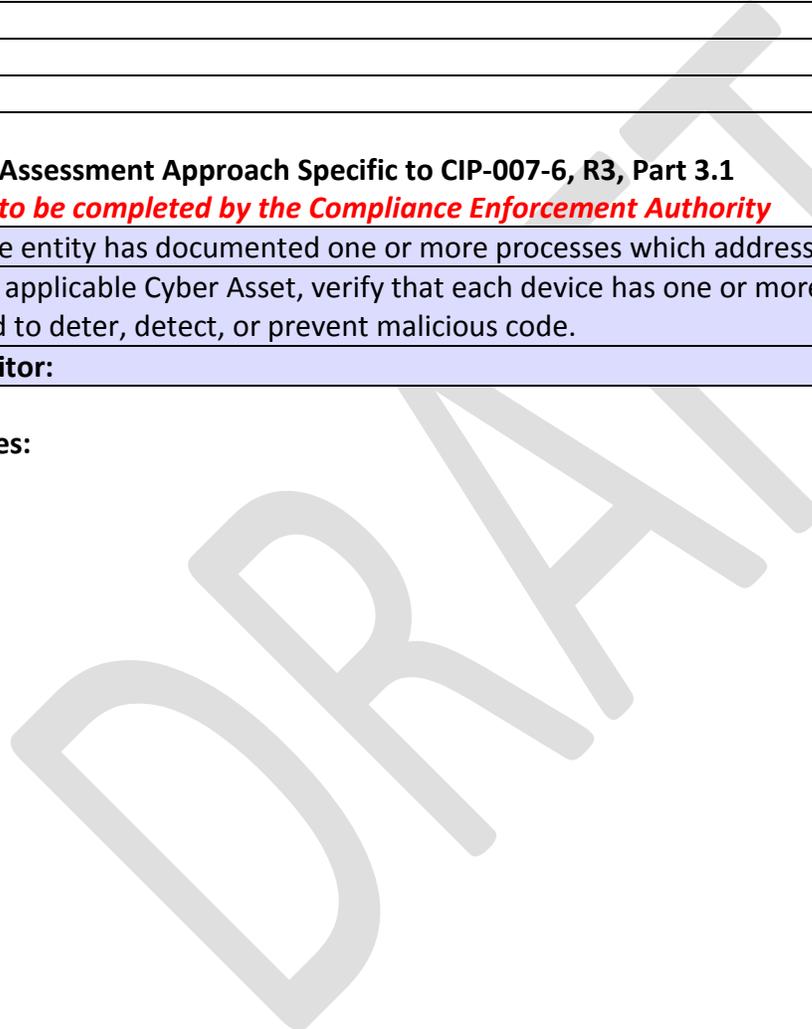
R3 Part 3.2

	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 R3 Part 3.2 applicable to this audit? ☐ Yes   ☐ No

If "No," why not?

☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-6, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more processes which address this Part.
	For each instance of detected malicious code, verify the malicious code was mitigated.
Note to Auditor:	

Auditor Notes:

R3 Part 3.3

<table>
<tr><td colspan="4" align="center">CIP-007-6 Table R3 – Malicious Code Prevention</td></tr>
<tr><td>Part</td><td align="center">Applicable Systems</td><td align="center">Requirements</td><td align="center">Measures</td></tr>
<tr>
<td>3.3</td>
<td>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</td>
<td>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.</td>
<td>An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.</td>
</tr>
</table>

Registered Entity Response (Required):

Question: Is R3 Part 3.3 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-007-6, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more processes which address this Part.
	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.
Note to Auditor:	

Auditor Notes:

_____

DRAFT NERC Reliability Standard Audit Worksheet
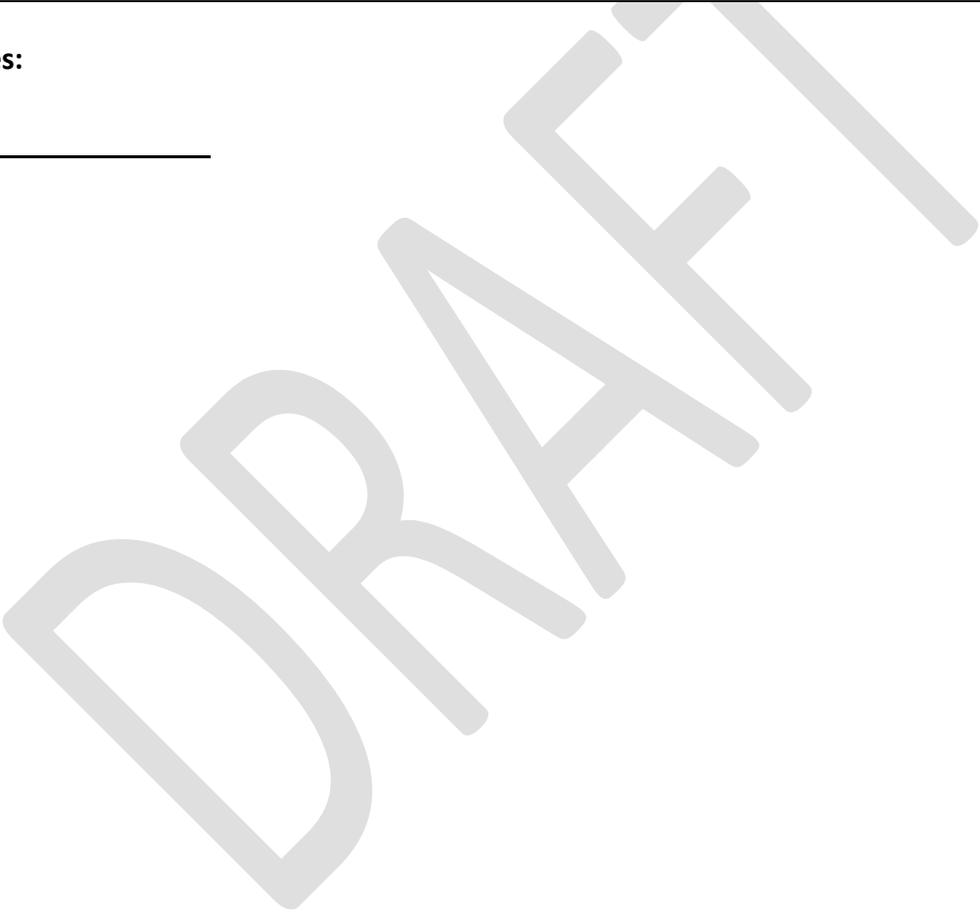
R4 Supporting Evidence and Documentation

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.

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

	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 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, EACMS, PACS, or PCA is capable of, and configured for, logging the event type; or
	    b. The BES Cyber System, EACMS, PACS, or PCA is not capable of logging the event type.
	 2. Verify logs of configured events are being generated by the BES Cyber System, EACMS, PACS, or PCA.

	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 is capable of, and configured for, logging the event type; or
	    b. The Cyber Asset is not capable of logging the event type.
	 2. Verify logs of configured events are being generated by the Cyber Asset.

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.

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**

DRAFT NERC Reliability Standard Audit Worksheet
Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD
RSAW Version: RSAW CIP-007-6 DRAFT2v0   Revision Date: September 17, 2014   RSAW Template: RSAW2014R1.3

25

DRAFT NERC Reliability Standard Audit Worksheet

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

	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.
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.

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

	Verify the entity has documented one or more processes which address this Part.
	For each BES Cyber System and 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.
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.

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

	Verify the entity has documented one or more processes which address this Part.
	Verify the entity reviews a summary or sampling of logged events at least every 15 calendar days to identify otherwise undetected Cyber Security Incidents.
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.

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

	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.
	For each applicable BES Cyber System and the associated EACMS, PACS, and PCA, 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.
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.

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

	Verify the entity has documented one or more processes which address this Part.
	For each applicable Cyber Asset, verify the 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.
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.

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

DRAFT NERC Reliability Standard Audit Worksheet
Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD
RSAW Version: RSAW CIP-007-6 DRAFT2v0   Revision Date: September 17, 2014   RSAW Template: RSAW2014R1.3

36

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

	Verify the entity has documented one or more processes which address this Part.
	For each applicable Cyber Asset, verify the entity has identified individuals with authorized access to shared accounts.
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.

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):

DRAFT NERC Reliability Standard Audit Worksheet
Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD
RSAW Version: RSAW CIP-007-6 DRAFT2v0   Revision Date: September 17, 2014   RSAW Template: RSAW2014R1.3

38

Compliance Assessment Approach Specific to CIP-007-6, R5, Part 5.4
This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more processes which address this Part.
	For applicable Cyber Assets with the ability to change default passwords, verify the entity has changed the known default passwords.
	For applicable Cyber Assets that do not have the ability to change default passwords, verify the inability to do so.
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.

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-007-6, R5, Part 5.5
This section to be completed by the Compliance Enforcement Authority

	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, per 5.5.1.
	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:
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.

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.

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

	Verify the entity has documented one or more processes which address this Part.
	For applicable Cyber Assets, 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.
	For applicable Cyber Assets, 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.

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.

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.

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

	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.
Note to Auditor:	

Auditor Notes:
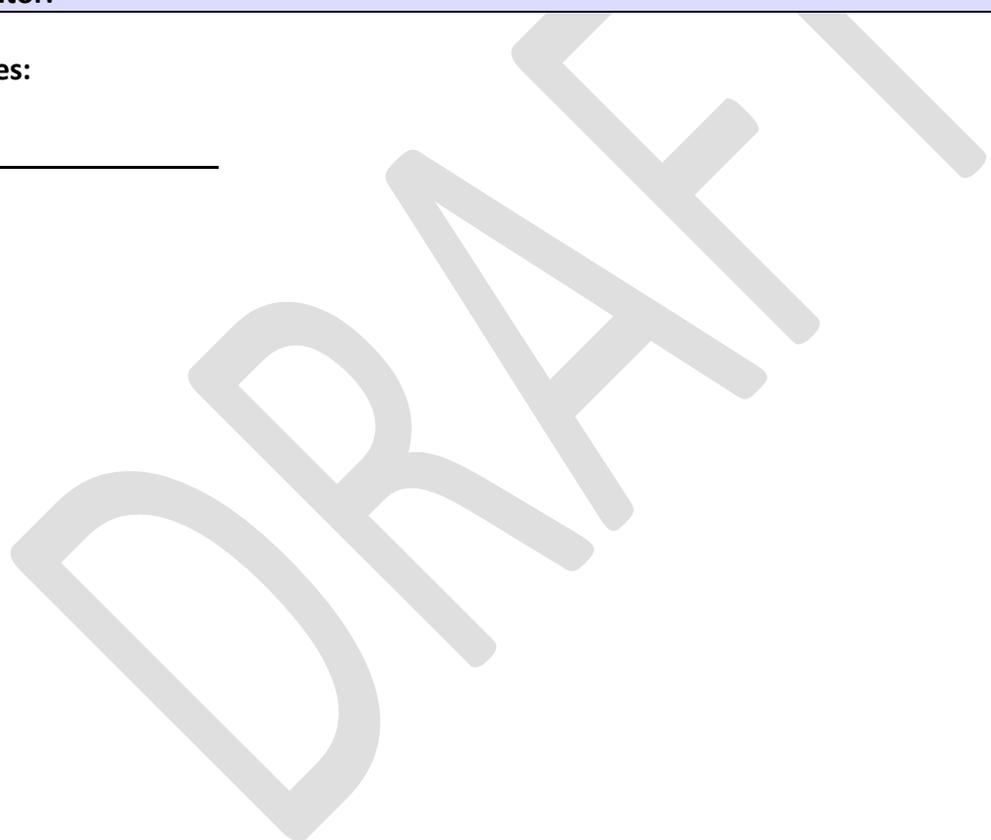
Additional Information:

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

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1v0	06/17/2014	Posted for Public Comment	New Document
Draft2v0	09/17/2014	CIP RSAW Development Team	Address comments received in response to Draft1v0.