

Reliability Standard Audit Worksheet¹

CIP-004-6 – Cyber Security – Personnel & Training

This section to be completed by the Compliance Enforcement Authority.

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

Applicability of Requirements

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

Legend:

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

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

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

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

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			
R2			
P2.1			
P2.2			
P2.3			
R3			
P3.1			
P3.2			
P3.3			
P3.4			
P3.5			
R4			
P4.1			
P4.2			
P4.3			
P4.4			
R5			
P5.1			
P5.2			
P5.3			
P5.4			
P5.5			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

DRAFT NERC Reliability Standard Audit Worksheet

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)

DRAFT

R1 Supporting Evidence and Documentation

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-004-6 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: <ul style="list-style-type: none"> • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

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

DRAFT NERC Reliability Standard Audit Worksheet

evidence, including links to the appropriate page, are recommended.

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documentation of a security awareness program for implementation of this Part.
Evidence of the implementation of the security awareness program for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.
Evidence that the security awareness program reinforces cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems at least every quarter.

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-004-6 R1 Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Requirement to this entity. If the Requirement is not applicable, skip the remaining items in this list.
	Review each security awareness program and verify that: <ol style="list-style-type: none"> The security awareness program is documented. The security awareness program has methods to reinforce cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.
	Verify that personnel receive on-going reinforcement in security practices.
	Verify the process(s) collectively reinforce cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems at least

DRAFT NERC Reliability Standard Audit Worksheet

	once every calendar quarter.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: 1.	

Auditor Notes:

DRAFT

R2 Supporting Evidence and Documentation

- R2.** Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M2.** Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

R2 Part 2.1

CIP-004-6 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Training content on: <ol style="list-style-type: none"> 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media. 	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

Registered Entity Response (Required):

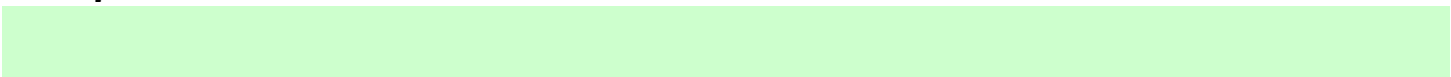
Question: Is R2.1 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]



DRAFT NERC Reliability Standard Audit Worksheet

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documentation of a cyber security training program(s) for implementation of this Part.
Content of each training program or module.
Description of the individual roles, functions, or responsibilities used to determine the applicability of each training program or module.
Evidence of how the entity determines who receives the training based on individual roles, functions, or responsibilities.

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-004-6 R2 Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the entity considers individual roles, functions, or responsibilities when implementing its training program(s).
	Verify that the training program for each role, function, or responsibility includes appropriate content on all of the following: <ul style="list-style-type: none"> • Cyber security policies; • Physical access controls;

DRAFT NERC Reliability Standard Audit Worksheet

	<ul style="list-style-type: none">• Electronic access controls;• The visitor control program;• Handling of BES Cyber System Information and its storage;• Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;• Recovery plans for BES Cyber Systems;• Response to Cyber Security Incidents; and• Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: 1.	

Auditor Notes:

DRAFT

R2 Part 2.2

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

Registered Entity Response (Required):

Question: Is R2.2 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
If an exception to this part was taken during CIP Exceptional Circumstances, describe the nature and duration of the exception.
Evidence Set 1:

DRAFT NERC Reliability Standard Audit Worksheet

1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of employment (i.e., employee, contractor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of employment (i.e., employee, contractor)
 - d. Role, function, or responsibilities
 - e. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - f. Date(s) of training for access during the audit period (may include dates prior to the audit period to establish initial compliance)
 - g. For each training date, the type of training (role, function, or responsibility-based programs, modules, etc.) performed
 - h. Evidence of training (e.g., class attendance sheets, logs of computer-based training, etc.)

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

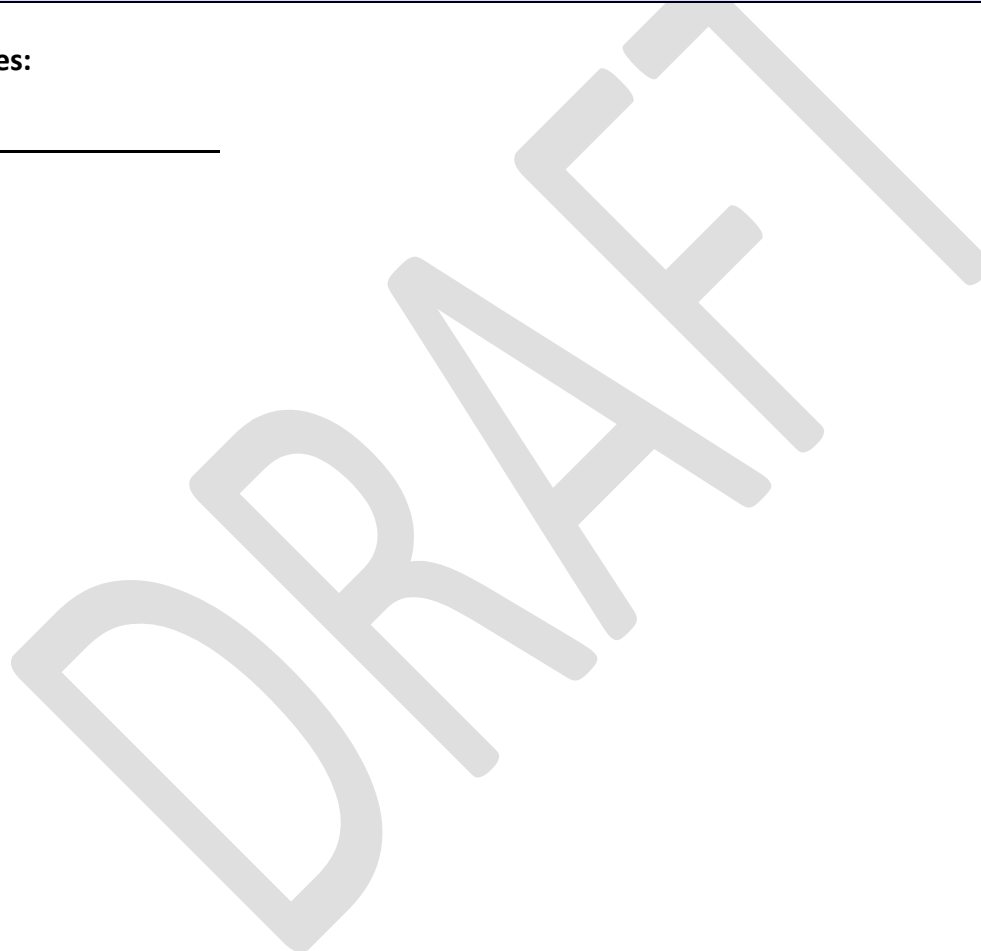
Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6 R2 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify training for sampled personnel has been conducted prior to being granted authorized electronic access and/or authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.
	Verify training appropriate to each person's role, function, or responsibilities was conducted.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.	

Auditor Notes:



R2 Part 2.3

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> • EACMS; and • PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Registered Entity Response (Required):

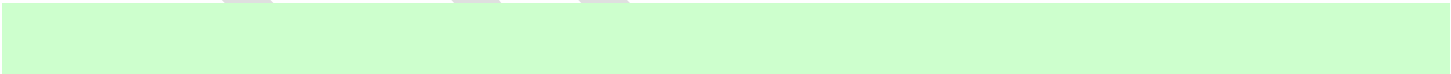
Question: Is R2.3 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

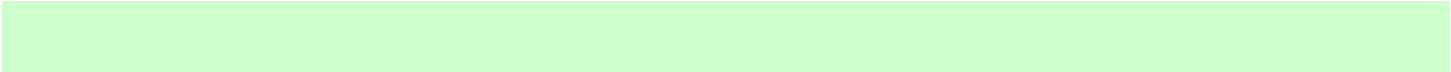
[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]



Registered Entity Response (Required):

Compliance Narrative:

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



Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1:

DRAFT NERC Reliability Standard Audit Worksheet

1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of employment (i.e., employee, contractor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of employment (i.e., employee, contractor)
 - d. Role, function, or responsibilities
 - e. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - f. Date(s) of training for access during the audit period (may include dates prior to the audit period to establish initial compliance)
 - g. For each training date, the type of training (role, function, or responsibility-based programs, modules, etc.) performed
 - h. Evidence of training (e.g., class attendance sheets, logs of computer-based training, etc.)

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-004-6 R2 Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify training for sampled personnel has been conducted at least once every 15 calendar months.
	Verify training appropriate to each person's role, function, or responsibilities was conducted.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	
1.	

Auditor Notes:

DRAFT

R3 Supporting Evidence and Documentation

- R3.** Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]
- M3.** Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

R3 Part 3.1

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to confirm identity.

Registered Entity Response (Required):

Question: Is R3.1 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference 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

DRAFT NERC Reliability Standard Audit Worksheet

evidence, including links to the appropriate page, are recommended.

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable personnel risk assessment programs for implementation of this Part.
For each personnel risk assessment program, indicate the applicability of each program.
Evidence Set 1: <ol style="list-style-type: none"> 1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual: <ol style="list-style-type: none"> a. Unique identifier (e.g., full name, employee number, etc.) b. Type of access granted (i.e., electronic, physical, both) c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of personnel to be used for the evidence requested below:
Evidence Set 2: <ol style="list-style-type: none"> 1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of employees. For each person in this sample set, provide the following: <ol style="list-style-type: none"> a. Unique identifier (e.g., full name, employee number, etc.) b. Type of access granted (i.e., electronic, physical, both) c. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact) d. Date(s) of personnel risk assessment(s) for access during the audit period (may include dates prior to the audit period to establish initial compliance) e. Evidence that the process to confirm identity in the applicable personnel risk assessment process was implemented

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

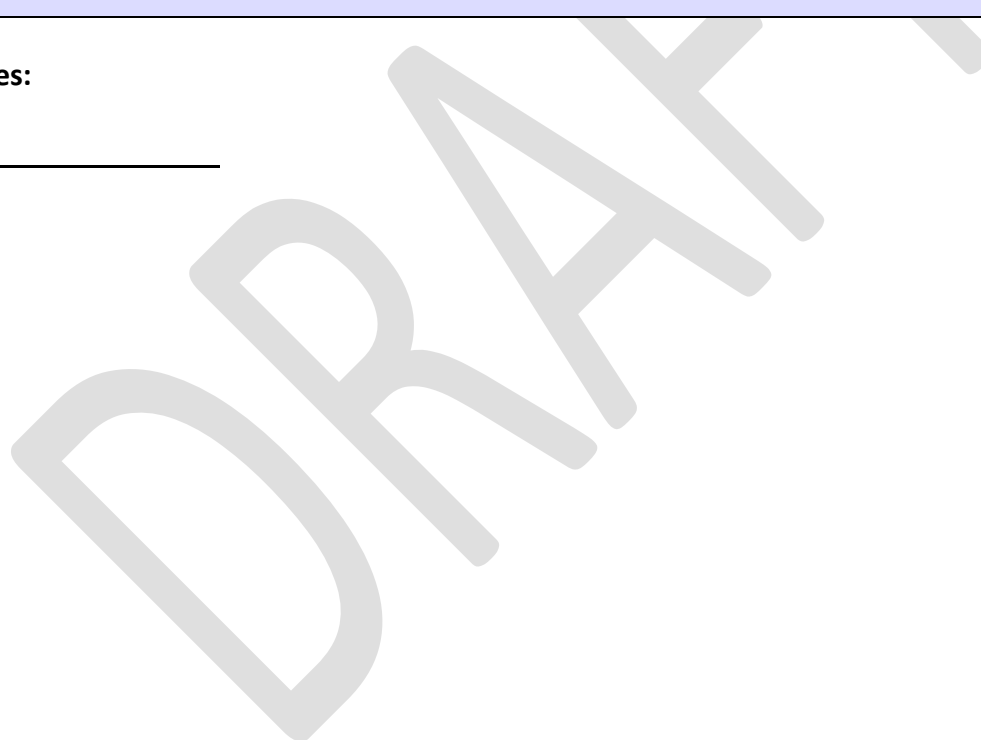
Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6 R3 Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that includes a process to confirm identity.
	For the sampled personnel, verify the applicable process to confirm identity was implemented in each case.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	
1.	

Auditor Notes:



R3 Part 3.2

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <p>3.2.1 current residence, regardless of duration; and</p> <p>3.2.2 other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.</p> <p>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to perform a seven year criminal history records check.</p>

Registered Entity Response (Required):

Question: Is R3.2 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

DRAFT NERC Reliability Standard Audit Worksheet

Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD

RSAW Version: RSAW CIP-004-6 DRAFT1v0 Revision Date: June 17, 2014 RSAW Template: RSAW2014R1.3

DRAFT NERC Reliability Standard Audit Worksheet

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable personnel risk assessment programs for implementation of this Part.
For each personnel risk assessment program, indicate the applicability of each program.
Evidence Set 1: <ol style="list-style-type: none"> 1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual: <ol style="list-style-type: none"> a. Unique identifier (e.g., full name, employee number, etc.) b. Type of access granted (i.e., electronic, physical, both) c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of personnel to be used for the evidence requested below:
Evidence Set 2: <ol style="list-style-type: none"> 1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of employees. For each person in this sample set, provide the following: <ol style="list-style-type: none"> a. Unique identifier (e.g., full name, employee number, etc.) b. Type of access granted (i.e., electronic, physical, both) c. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact) d. Date(s) of personnel risk assessment(s) for access during the audit period (may include dates prior to the audit period to establish initial compliance) e. Evidence that the process to seven year criminal history records check in the applicable personnel risk assessment process was implemented f. If a full seven year criminal history records check was not performed, provide documentation of the reason the full seven year criminal history records check could not be performed

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)	Description of Applicability of Document
-----------	----------------	---------------------------	------------------	---------------------	---

DRAFT NERC Reliability Standard Audit Worksheet

				or Section(s)	

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

Compliance Assessment Approach Specific to CIP-004-6 R3 Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that includes a process to perform a seven year criminal history records check that includes: <ol style="list-style-type: none"> 1. current residence, regardless of duration; and 2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.
	For the sampled personnel, verify the applicable process to perform a seven year criminal history records check was implemented in each case.
	For the sampled personnel, verify: <ul style="list-style-type: none"> • A full seven year criminal history records check was completed, or • A full seven year criminal history records check was not completed and: <ol style="list-style-type: none"> 1. The reason the check was not completed is documented, and 2. It was not possible for the entity to perform a full seven year criminal history records check.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	
1.	

Auditor Notes:

R3 Part 3.3

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

Registered Entity Response (Required):

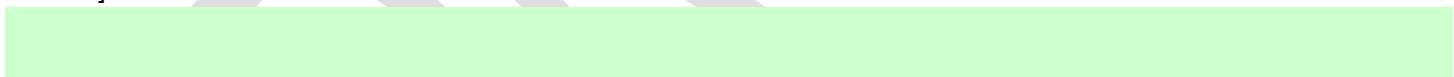
Question: Is R3.3 applicable to this audit? Yes No

If "No," why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

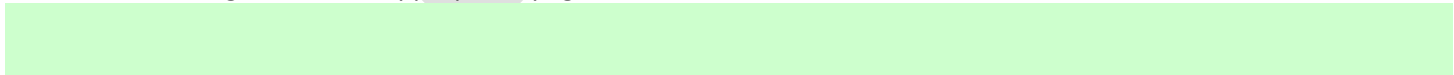
[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]



Registered Entity Response (Required):

Compliance Narrative:

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



Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable personnel risk assessment programs for implementation of this Part.
For each personnel risk assessment program, indicate the applicability of each program.
Evidence Set 1:
1. List of all individuals who were granted authorized electronic access, authorized unescorted physical

DRAFT NERC Reliability Standard Audit Worksheet

access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual:

- a. Unique identifier (e.g., full name, employee number, etc.)
- b. Type of access granted (i.e., electronic, physical, both)
- c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of employees. For each person in this sample set, provide the following:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - d. Date(s) of personnel risk assessment(s) for access during the audit period (may include dates prior to the audit period to establish initial compliance)
 - e. Evidence that criminal history records checks were evaluated per the criteria or process included in the applicable personnel risk assessment program.

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-004-6 R3 Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber
--	---

DRAFT NERC Reliability Standard Audit Worksheet

	Systems that includes criteria or a process to evaluate criminal history records checks for authorizing access.
	For the sampled personnel, verify the applicable criteria or process to evaluate criminal history records checks for authorizing access was implemented in each case.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: 1.	

Auditor Notes:

DRAFT

R3 Part 3.4

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments.

Registered Entity Response (Required):

Question: Is R3.4 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable personnel risk assessment programs for implementation of this Part.
For each personnel risk assessment program, indicate the applicability of each program.
Evidence Set 1:

DRAFT NERC Reliability Standard Audit Worksheet

1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of contractors and service vendors. For each person in this sample set, provide the following:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - d. Date(s) of personnel risk assessment(s) for access during the audit period (may include dates prior to the audit period to establish initial compliance)
 - e. Evidence that the criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3 was implemented.

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-004-6 R3 Part 3.4

DRAFT NERC Reliability Standard Audit Worksheet

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that includes criteria or a process to verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
	For the sampled personnel, verify the applicable criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3 was implemented.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: 1.	

Auditor Notes:

DRAFT

R3 Part 3.5

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Registered Entity Response (Required):

Question: Is R3.5 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable personnel risk assessment programs for implementation of this Part.
For each personnel risk assessment program, indicate the applicability of each program.
Evidence Set 1:

DRAFT NERC Reliability Standard Audit Worksheet

1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - d. Date(s) of personnel risk assessment(s) for access during the audit period (may include dates prior to the audit period to establish initial compliance)
 - e. Evidence of completion of the personnel risk assessment process on the dates listed

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-004-6 R3 Part 3.5

This section to be completed by the Compliance Enforcement Authority

	For the sampled personnel, verify the applicable personnel risk assessment process was implemented in each case at least once every seven years.
--	--

DRAFT NERC Reliability Standard Audit Worksheet

	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: 1.	

Auditor Notes:

DRAFT

R4 Supporting Evidence and Documentation

- R4.** Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].
- M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

R4 Part 4.1

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: <ol style="list-style-type: none"> 4.1.1 Electronic access; 4.1.2 Unescorted physical access into a Physical Security Perimeter; and 4.1.3 Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. 	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Registered Entity Response (Required):

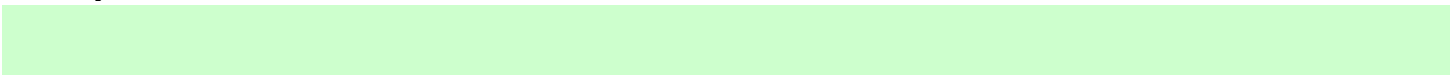
Question: Is R4.1 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]



DRAFT NERC Reliability Standard Audit Worksheet

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.

All applicable access management programs for implementation of this Part

For each access management program, indicate the applicability of each program

If any access management program for an Applicable System has experienced an exception for CIP Exceptional Circumstances, provide evidence describing these circumstances, including any applicable cyber security policies

Evidence Set 1:

1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - d. Authorization records (granting access to any of the Applicable Systems, or to BES Cyber System Information pertaining to any of the Applicable Systems) for electronic access, unescorted physical access into a PSP, and access to designated storage locations for BES Cyber System Information
 - e. For each Applicable System for which the person was authorized access, provide evidence of the actual permissions granted to this person
 - f. Evidence that the applicable access management program was implemented to grant access

Registered Entity Evidence (Required):

DRAFT NERC Reliability Standard Audit Worksheet

Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD

RSAW Version: RSAW CIP-004-6 DRAFT1v0 Revision Date: June 17, 2014 RSAW Template: RSAW2014R1.3

DRAFT NERC Reliability Standard Audit Worksheet

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-004-6 R4 Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more access management programs.
	If the entity has experienced an exception for CIP Exceptional Circumstances, verify the entity has adhered to any applicable cyber security policies.
	For the sampled personnel, verify the entity’s access management programs authorize access based on need.
	For the sampled personnel, verify the entity keeps records of authorizations.
	For the sampled personnel, verify the entity’s authorizations match the access granted.
	For the sampled personnel, verify the entity’s applicable access management programs were implemented to grant access.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	
1.	

Auditor Notes:

R4 Part 4.2

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Registered Entity Response (Required):

Question: Is R4.2 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

DRAFT NERC Reliability Standard Audit Worksheet

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response **(Required)**:

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.

All applicable access management programs for implementation of this Part

For each access management program, indicate the applicability of each program

Evidence Set 1:

1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the applicable Cyber Assets during the audit period. Provide the following for each individual:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following:
 - d. Unique identifier (e.g., full name, employee number, etc.)
 - e. Type of access granted (i.e., electronic, physical, both)
 - f. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - g. Evidence of verification of authorization records performed during the audit period

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.

DRAFT NERC Reliability Standard Audit Worksheet

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-004-6 R4 Part 4.2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity’s access management programs require quarterly verification of authorization records.
	For the sampled personnel, verify the entity has implemented the applicable access management program for verification of authorization records at least once each calendar quarter during the audit period.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	
1.	

Auditor Notes:

R4 Part 4.3

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.</p>	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Registered Entity Response (Required):

Question: Is R4.3 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

DRAFT NERC Reliability Standard Audit Worksheet

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable access management programs for implementation of this Part
For each access management program, indicate the applicability of each program
Evidence Set 1: 1. List of all individuals who were granted authorized electronic access to any of the applicable Cyber Assets during the audit period. Provide the following for each individual: a. Unique identifier (e.g., full name, employee number, etc.) b. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of personnel to be used for the evidence requested below:
Evidence Set 2: 1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following: a. Unique identifier (e.g., full name, employee number, etc.) b. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact) c. Evidence of verification of correct implementation of user accounts, user account groups, or user role categories, and their specific, associated privileges during the audit period. d. Evidence of verification of the necessity of authorized privileges during the audit period.

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)	Description of Applicability of Document
-----------	----------------	---------------------	---------------	------------------	--

DRAFT NERC Reliability Standard Audit Worksheet

				or Section(s)	

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

Compliance Assessment Approach Specific to CIP-004-6 R4 Part 4.3

This section to be completed by the Compliance Enforcement Authority

	Verify the entity’s access management programs require verification of correct implementation of user accounts, user account groups, or user role categories, and their specific, associated privileges at least every 15 calendar months.
	For the sampled personnel, verify the entity has performed verification of correct implementation of user accounts, user account groups, or user role categories, and their specific, associated privileges at least every 15 calendar months.
	For the sampled personnel, verify the entity has performed verification of the necessity of authorized privileges at least every 15 calendar months.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

- 1.

Auditor Notes:

R4 Part 4.4

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.</p>	<p>An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Registered Entity Response (Required):

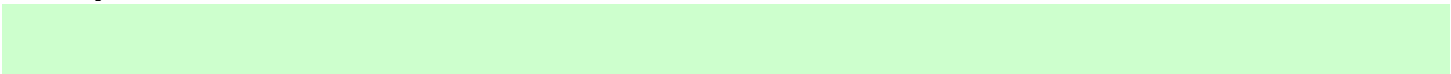
Question: Is R4.4 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]



DRAFT NERC Reliability Standard Audit Worksheet

Registered Entity Response **(Required)**:

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.

All applicable access management programs for implementation of this Part

For each access management program, indicate the applicability of each program

List of all designated storage locations for BES Cyber System Information, including a designation of whether the location is electronic or physical

Evidence Set 1:

1. List of all individuals who were granted authorized electronic access, authorized unescorted physical access, or both, to any of the designated storage locations for BES Cyber System Information during the audit period. Provide the following for each individual:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Type of personnel (i.e., employee, contractor, service vendor)

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following:
 - a. Unique identifier (e.g., full name, employee number, etc.)
 - b. Type of access granted (i.e., electronic, physical, both)
 - c. Date each type of access was granted (if prior to the CIP-004-6 effective date for this entity, "Legacy" may be used to indicate this fact)
 - d. Evidence of verification during the audit period that access permissions to designated storage locations for BES Cyber System Information are correct.
 - e. Evidence of verification of the necessity of authorized privileges during the audit period.

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.

DRAFT NERC Reliability Standard Audit Worksheet

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-004-6 R4 Part 4.4

This section to be completed by the Compliance Enforcement Authority

	Verify the entity’s access management programs require verification that access permissions to designated storage locations for BES Cyber System Information are correct at least every 15 calendar months.
	For the sampled personnel, verify the entity has performed verification that access permissions to designated storage locations for BES Cyber System Information are correct at least every 15 calendar months.
	For the sampled personnel, verify the entity has performed verification of the necessity of authorized privileges at least every 15 calendar months.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	
1.	

Auditor Notes:

R5 Supporting Evidence and Documentation

- R5.** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R5 Part 5.1

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

Registered Entity Response (Required):

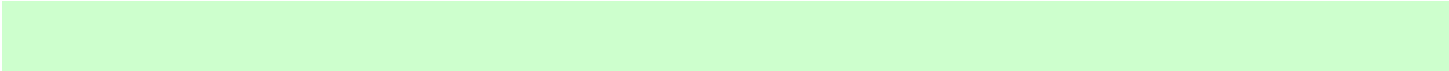
Question: Is R5.1 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]



Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable access revocation programs for implementation of this Part
For each access revocation program, indicate the applicability of each program
Evidence Set 1: 1. For the audit period, provide a list of all termination actions of personnel with authorized electronic access or authorized unescorted physical access to any of the Applicable Systems, or authorized access to BES Cyber System Information. Include the following information for each termination action: a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual's name is not required information) b. Type of personnel (i.e., employee, contractor, service vendor) c. Type of authorized access: i. Authorized unescorted physical access ii. Authorized electronic access iii. Interactive Remote Access iv. Access to repositories of BES Cyber System Information v. Knowledge of shared account passwords for Applicable Systems

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of personnel to be used for the evidence requested below:
Evidence Set 2: 1. From the list of termination actions provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of termination actions of personnel with authorized unescorted physical access or Interactive Remote Access. For each termination action in this sample set, provide the following: a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual's name is not required information) b. Type of personnel (i.e., employee, contractor, service vendor) c. Type of authorized access: i. Authorized unescorted physical access ii. Interactive Remote Access d. List of BES Cyber Systems and/or Cyber Assets to which the individual had authorized access e. Effective date and time of the termination action f. If the individual had authorized unescorted physical access:

DRAFT NERC Reliability Standard Audit Worksheet

- i. Evidence of the date and time the removal of the individual’s ability for authorized unescorted physical access was completed
- ii. The method used for the removal
- g. If the individual had the ability for Interactive Remote Access:
 - i. Evidence of the date and time the removal of the individual’s ability for Interactive Remote Access was completed
 - ii. The method used for the removal

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-004-6 R5 Part 5.1

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more access revocation programs.
	Verify that each applicable access revocation program contains a process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action.
	For the sampled termination actions, verify the removal of the ability for unescorted physical access and Interactive Remote Access within 24 hours of the termination action.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Removal of the ability for access does not necessarily require removal or disabling of the individual’s accounts. The ability for access may be removed by disabling the individual’s network access, confiscation of a badge, or other suitable means. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual’s multi-factor authentication.

Auditor Notes:

DRAFT

R5 Part 5.2

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Registered Entity Response (Required):

Question: Is R5.2 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.

DRAFT NERC Reliability Standard Audit Worksheet

All applicable access revocation programs for implementation of this Part

For each access revocation program, indicate the applicability of each program

Evidence Set 1:

1. For the audit period, provide a list of all reassignments or transfers of personnel with authorized electronic access or authorized unescorted physical access to any of the Applicable Systems. Include the following information for each reassignment or transfer:
 - a. Unique identifier for the individual (e.g., name, employee number, badge number, unique username, etc.)
 - b. Type of personnel (i.e., employee, contractor, service vendor)
 - c. Type of authorized access:
 - i. Authorized unescorted physical access
 - ii. Authorized electronic access

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of reassignments or transfers of personnel provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of personnel. For each person in this sample set, provide the following:
 - a. Unique identifier for the individual (e.g., name, employee number, badge number, unique username, etc.)
 - b. Type of personnel (i.e., employee, contractor, service vendor)
 - c. Type of authorized access:
 - i. Authorized unescorted physical access
 - ii. Authorized electronic access
 - d. List of BES Cyber Systems and/or Cyber Assets to which the individual had authorized access
 - e. Effective date of the reassignment or transfer
 - f. Date access determined to be no longer needed
 - g. If the individual had authorized unescorted physical access, evidence of the date of physical access revocation
 - h. If the individual had authorized electronic access, evidence of the date of electronic access revocation

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

Compliance Assessment Approach Specific to CIP-004-6 R5 Part 5.2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more access revocation programs.
	Verify that each applicable access revocation program contains a process to manage reassignments or transfers.
	For the sampled reassignments or transfers, verify the revocation of access by the end of the calendar day following determination that access is no longer required.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
	Review the applicable access revocation programs to determine whether the programs contain a process to revoke access to shared accounts upon reassignment or transfer of personnel. The auditor should document a Recommendation if this topic is not addressed.

Note to Auditor:

- 1.

Auditor Notes:

R5 Part 5.3

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

Registered Entity Response (Required):

Question: Is R5.3 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact or medium impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested¹:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable access revocation programs for implementation of this Part
For each access revocation program, indicate the applicability of each program

DRAFT NERC Reliability Standard Audit Worksheet

Evidence Set 1:

1. For the audit period, provide a list of all termination actions of personnel with authorized electronic access or authorized unescorted physical access to any of the Applicable Systems, or authorized access to BES Cyber System Information. Include the following information for each termination action:
 - a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual’s name is not required information)
 - b. Type of personnel (i.e., employee, contractor, service vendor)
 - c. Type of authorized access:
 - i. Authorized unescorted physical access
 - ii. Authorized electronic access
 - iii. Interactive Remote Access
 - iv. Access to repositories of BES Cyber System Information
 - v. Knowledge of shared account passwords for Applicable Systems

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of termination actions provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of termination actions of personnel with authorized access to designated storage locations (electronic or physical) for BES Cyber System Information. For each termination action in this sample set, provide the following:
 - a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual’s name is not required information)
 - b. Type of personnel (i.e., employee, contractor, service vendor)
 - c. Type of authorized access:
 - i. Physical access to BES Cyber System Information
 - ii. Electronic access to BES Cyber System Information
 - d. List of storage locations for BES Cyber System Information to which the individual had authorized access
 - e. Effective date of the termination action
 - f. Evidence of the date the revocation of the individual’s ability for physical and/or electronic access was completed

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

Compliance Assessment Approach Specific to CIP-004-6 R5 Part 5.3

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more access revocation programs.
	Verify that each applicable access revocation program contains a process to revoke an individual's physical or electronic access to BES Cyber System Information upon a termination action.
	For the sampled termination actions, verify the revocation of an individual's physical or electronic access to BES Cyber System Information by the end of the next calendar day following the effective date of the termination action.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

- 1.

Auditor Notes:

R5 Part 5.4

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Registered Entity Response (Required):

Question: Is R5.4 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable access revocation programs for implementation of this Part
For each access revocation program, indicate the applicability of each program
Evidence Set 1:

DRAFT NERC Reliability Standard Audit Worksheet

1. For the audit period, provide a list of all termination actions of personnel with authorized electronic access or authorized unescorted physical access to any of the Applicable Systems, or authorized access to BES Cyber System Information. Include the following information for each termination action:
 - a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual’s name is not required information)
 - b. Type of personnel (i.e., employee, contractor, service vendor)
 - c. Type of authorized access:
 - i. Authorized unescorted physical access
 - ii. Authorized electronic access
 - iii. Interactive Remote Access
 - iv. Access to repositories of BES Cyber System Information
 - v. Knowledge of shared account passwords for Applicable Systems

Additional Evidence Requested:

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

Evidence Set 2:

1. From the list of termination actions provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of termination actions of personnel with authorized electronic access. For each termination action in this sample set, provide the following:
 - a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual’s name is not required information)
 - b. Type of personnel (i.e., employee, contractor, service vendor)
 - c. List of non-shared user accounts to which the individual had access
 - d. Effective date of the termination action
 - e. Evidence of the date the revocation of the individual’s non-shared user accounts was completed

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

Compliance Assessment Approach Specific to CIP-004-6 R5 Part 5.4

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more access revocation programs.
	Verify that each applicable access revocation program contains a process to revoke an individual’s non-shared user accounts within 30 calendar days of the effective date of the termination action.
	For the sampled termination actions, verify the revocation of the individual’s non-shared user accounts within 30 calendar days of the effective date of the termination action.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: 1.	

Auditor Notes:



R5 Part 5.5

CIP-0046 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS	<p>For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p> <p>If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ol style="list-style-type: none"> 1. Workflow or sign-off form showing password reset within 30 calendar days of the termination; 2. Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or 3. Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Registered Entity Response (Required):

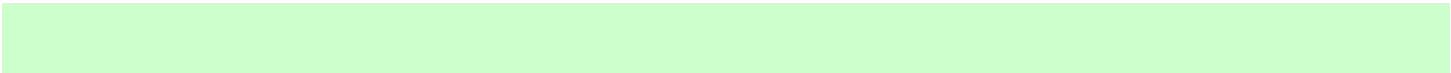
Question: Is R5.5 applicable to this audit? Yes No

If “No,” why not?

This entity does not have any high impact BES Cyber Systems.

Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]



DRAFT NERC Reliability Standard Audit Worksheet

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable access revocation programs for implementation of this Part
For each access revocation program, indicate the applicability of each program
Evidence Set 1: 1. For the audit period, provide a list of all termination actions of personnel with authorized electronic access or authorized unescorted physical access to any of the Applicable Systems, or authorized access to BES Cyber System Information. Include the following information for each termination action: a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual’s name is not required information) b. Type of personnel (i.e., employee, contractor, service vendor) c. Type of authorized access: i. Authorized unescorted physical access ii. Authorized electronic access iii. Interactive Remote Access iv. Access to repositories of BES Cyber System Information v. Knowledge of shared account passwords for Applicable Systems

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of personnel to be used for the evidence requested below:
Evidence Set 2: 1. From the list of termination actions provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of termination actions of personnel with knowledge of shared account passwords for Applicable Systems. For each termination action in this sample set, provide the following: a. Unique identifier for the terminated individual (e.g., employee number, badge number, unique username, etc.; note that the individual’s name is not required information) b. Type of personnel (i.e., employee, contractor, service vendor) c. Effective date of the termination action d. List of shared accounts to which the individual had access e. Evidence of the date the password change for each shared user account to which the individual had access was completed f. If the “extenuating operating circumstances” clause was invoked, documentation of the extenuating operating circumstances, including the date of the end of the extenuating

DRAFT NERC Reliability Standard Audit Worksheet

operating circumstances.

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-004-6 R5 Part 5.5

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more access revocation programs.
	Verify that each applicable access revocation program contains a process to change the passwords for shared accounts known to the terminated individual within 30 calendar days of the effective date of the termination action. The access revocation program may include provision for extenuating operating circumstances.
	If extenuating operating circumstances are invoked, verify the circumstances are documented and include a specific end date.
	For the sampled termination actions that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the terminated individual have been changed within 30 calendar days of the termination action.
	For the sampled termination actions that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the terminated individual have been changed within 10 calendar days following the end of the extenuating operating circumstances.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-004-6 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

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

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

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

Sampling Methodology

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

Regulatory Language

See FERC Order 706

See FERC Order 791

Selected Glossary Terms

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

Term	Acronym	Definition
BES Cyber Asset	BCA	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. A Transient Cyber Asset is not a BES Cyber Asset.

DRAFT NERC Reliability Standard Audit Worksheet

BES Cyber System		One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
BES Cyber System Information		Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
CIP Exceptional Circumstance		A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.
Cyber Assets		Programmable electronic devices, including the hardware, software, and data in those devices.
Cyber Security Incident		A malicious act or suspicious event that: <ul style="list-style-type: none"> • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.
Electronic Access Control or Monitoring Systems	EACMS	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.
External Routable Connectivity		The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
Interactive Remote Access		User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's

DRAFT NERC Reliability Standard Audit Worksheet

		Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
Physical Access Control Systems	PACS	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter	PSP	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Removable Media		Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.
Transient Cyber Asset		A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

DRAFT NERC Reliability Standard Audit Worksheet

Revision History for RSAW

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

¹ Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

DRAFT