NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-004-8 – 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	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		
R3	X	X	X	X		X			X	X		
R4	X	X	X	X		X			X	X		
R5	X	X	X	X		X			X	X		

Legend:

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

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

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

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

Findings

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

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			
R5			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

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

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

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 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-004-8 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-004-8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	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 Applicable 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: • 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include 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 Applicable Systems.
	Verify the Responsible Entity has reinforced security awareness at least once each calendar quarter.
	Verify the security awareness reinforcement included: • reinforcement of cyber security practices, or • reinforcement of physical security practices associated with cyber security.
	Verify that security awareness was reinforced for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.
Note to Auditor: The Responsible Entity is not required to document that each quarter's reinforcement was received by each of its authorized personnel. Rather, the Responsible Entity is required to demonstrate that the security awareness reinforcement was communicated to its authorized personnel as a whole, not necessarily individually.	

Auditor Notes:

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-004-8 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-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

R2 Part 2.1

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 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 (BCSI) 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 BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the training program(s) collectively include content on the following: 1. Cyber security policies; 2. Physical access controls; 3. Electronic access controls; 4. The visitor control program; 5. Handling of BCSI and its storage; 6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 7. Recovery plans for BCS; 8. Response to Cyber Security Incidents; and 9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including TCA, and with Removable Media.
	Verify the Responsible Entity's training program's content is appropriate to individual roles, functions, or responsibilities.
Notes to Auditor: 1. The training program(s) must collectively include all nine training elements. 2. It is not necessary that all nine training elements be included for the training of each role, function, or responsibility. 3. Each role, function, or responsibility must receive training on all appropriate training elements.	

Auditor Notes:

R2 Part 2.2

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-004-8, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel completed the training specified in Part 2.1 prior to being granted authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R2 Part 2.3

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated individual training records.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel with authorized electronic access or authorized unescorted physical access to applicable Cyber Assets completed the training specified in Part 2.1 at least once every 15 calendar months, (except for medium impact BCS without ERC).

Auditor Notes:

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 Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 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-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

R3 Part 3.1

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.1
This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include a process to confirm identity.
	Verify a process to confirm identity was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.2

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1 current residence, regardless of duration; and 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. 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 could not be performed.	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.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include a process to perform a seven year criminal history records check that includes: 1. current residence, regardless of duration; 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; and 3. performing as much of the seven year criminal history records check as possible, if it is not possible to perform a full seven year criminal history records check.
	Verify a process to perform a seven year criminal history records check was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems and: • A full seven year criminal history records check was completed; or • The Responsible Entity completed as much of the seven year criminal history records check as possible, and documented the reason the full seven year criminal history records check was not completed.

Auditor Notes:

R3 Part 3.3

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	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 criteria or process to evaluate criminal history records checks.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include criteria or a process to evaluate criminal history records checks for authorizing access.
	Verify the applicable criteria or process to evaluate criminal history records checks for authorizing access was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.4

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with IRA SCI supporting an Applicable System in this Part	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.	Examples of evidence may include, but are 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include criteria or a process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
	Verify 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.

Auditor Notes:

R3 Part 3.5

CIP-004-86 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.5

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include a process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.
	For personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems, verify the applicable personnel risk assessment process was implemented at least once every seven years.

Auditor Notes:

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-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [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-004-8 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-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1 Electronic access; 4.1.2 Unescorted physical access into a Physical Security Perimeter (PSP)(except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs which include a process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 1. Electronic access; and 2. unescorted physical access into a PSP
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
	Verify access was authorized, based on need, for: 1. Electronic access; and 2. unescorted physical access into a PSP
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R4 Part 4.2

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-004-8, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs which include a process to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.
	Verify the Responsible Entity has verified at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

Auditor Notes:

R4 Part 4.3

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	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.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs that, 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.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that 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.

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-004-8 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-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R5 Part 5.1

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for Medium impact BCS without ERC) and Interactive Remote Access (IRA) 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).	An example of evidence may include, but is not limited to, documentation of all of the following: 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs that include a process to initiate removal of an individual's ability for unescorted physical access and IRA 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).
	Verify the Responsible Entity has: 1. initiated removal of an individual's ability for unescorted physical access and IRA upon a termination action; and 2. completed 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).
Note to Auditor: 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 IRA may be accomplished, for example, by disabling the individual's multi-factor authentication.	

Auditor Notes:

R5 Part 5.2

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for Medium impact BCS without ERC) 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.	Examples of evidence may include, but are not limited to, documentation of all of the following: 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for reassignments or transfers to 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.
	Verify the Responsible Entity has, for reassignments or transfers, revoked 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.
Note to Auditor: Revocation of access does not necessarily require removal of the individual's accounts. The account may be disabled in lieu of removal.	

Auditor Notes:

R5 Part 5.3

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Examples of evidence may include, but are 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 revocation of access and dated within thirty calendar days of the termination actions.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination actions to revoke the individual's non-shared user accounts (unless already revoked according to Requirement R5, Part 5.1), within 30 calendar days of the effective date of the termination action.
	Verify the Responsible Entity has, for termination actions, revoked the individual's non-shared user accounts (unless already revoked according to Requirement R5.1), within 30 calendar days of the effective date of the termination action.

Notes to Auditor:

1. If the access was already revoked under the actions taken for Requirement R5, Part 5.1, no further action is needed.
2. Revocation of 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.
3. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual's multi-factor authentication.

Auditor Notes:

R5 Part 5.4

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	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. 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.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action. • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • 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):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination actions to 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. The documented process(es) may include provisions for the Responsible Entity to determine and document that extenuating operating circumstances require a longer time period, and may change the password(s) within 10 calendar days following the end of the operating circumstances.
	If extenuating operating circumstances are invoked, verify the circumstances are documented and include a specific end date.
	For termination actions that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the termination action.
	For termination actions that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.
	For reassignments or transfers that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the date that the Responsible Entity determines the individual no longer requires retention of the access.
	For reassignments or transfers that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004- 8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R6 Part 6.1

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R6, Part 6.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more BCSI access management programs that include a process to, prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 1. Provisioned electronic access to electronic BCSI; and 2. Provisioned physical access to physical BCSI.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
	Verify the Responsible Entity has, prior to provisioning, authorized (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 1. Provisioned electronic access to electronic BCSI; and 2. Provisioned physical access to physical BCSI.

Auditor Notes:

R6 Part 6.2

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

Compliance Assessment Approach Specific to CIP-004-8, R6, Part 6.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more BCSI access management programs that include a process to verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.
	Verify the Responsible Entity has verified at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.

Auditor Notes:

R6 Part 6.3

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a Medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-004-8, R6, Part 6.3
This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has, for termination actions, documented one or more BCSI access management programs that include a process to remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.
	Verify the Responsible Entity has, for termination actions, removed the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-004-8 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

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

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

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

Sampling Methodology

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

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	02/28/2024		Initial Draft