

Reliability Standard Audit Worksheet¹

CIP-006-6 – Cyber Security – Security Management Controls

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		

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			
P1.2			
P1.3			
P1.4			
P1.5			
P1.6			
P1.7			
P1.8			
P1.9			
P1.10			
R2			
P2.1			
P2.2			
P2.3			
R3			
P3.1			

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

DRAFT NERC Reliability Standard Audit Worksheet

R1 Supporting Evidence and Documentation

- R1.** Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].
- M1.** Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

R1 Part 1.1

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

Registered Entity Response (Required):

Question: Is R1 Part 1.1 applicable to this audit? Yes No

If “No,” why not?

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted

DRAFT NERC Reliability Standard Audit Worksheet

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-006-6, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans that define operational or procedural controls to restrict physical access.
	Verify the Responsible Entity has implemented the defined operational or procedural controls to restrict physical access to Applicable Systems.

Auditor Notes:

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.2

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

Registered Entity Response (Required):

Question: Is R1 Part 1.2 applicable to this audit? Yes No

If “No,” why not?

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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-006-6, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans that utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.
	Verify that each PSP has at least one physical access control.
	Verify that only those individuals with authorized unescorted physical access are allowed unescorted physical access into each applicable PSP.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.3

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

Registered Entity Response (Required):

Question: Is R1 Part 1.3 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

DRAFT NERC Reliability Standard Audit Worksheet

Compliance Assessment Approach Specific to CIP-006-6, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans that utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, where technically feasible.
	Verify that each PSP has at least two physical access control, or that an approved TFE exists.
	Verify that only those individuals with authorized unescorted physical access are allowed authorized unescorted physical access into each applicable PSP.
	If a TFE is applicable, verify the compensating measures identified by the TFE are in place.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.4

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> EACMS; and PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> EACMS; and PCA 	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

Registered Entity Response (Required):

Question: Is R1 Part 1.4 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

DRAFT NERC Reliability Standard Audit Worksheet

--

Compliance Assessment Approach Specific to CIP-006-6, R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans to monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
	Verify that the Responsible Entity monitors for unauthorized access through a physical access point into a Physical Security Perimeter.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.5

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

Registered Entity Response (Required):

Question: Is R1 Part 1.5 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

DRAFT NERC Reliability Standard Audit Worksheet

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

Compliance Assessment Approach Specific to CIP-006-6, R1, Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans to issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.
	Verify that an alarm or alert is issued in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.6

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.6	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

Registered Entity Response (Required):

Question: Is R1 Part 1.6 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

Compliance Assessment Approach Specific to CIP-006-6, R1, Part 1.6

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.
	Verify that each Physical Access Control System is monitored for unauthorized physical access to a Physical Access Control System.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.7

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.7	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

Registered Entity Response (Required):

Question: Is R1 Part 1.7 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

--

DRAFT NERC Reliability Standard Audit Worksheet

Compliance Assessment Approach Specific to CIP-006-6 R1 Part 1.7

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans to issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.
	Verify that an alarm or alert is issued in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.8

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.8	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

Registered Entity Response (Required):

Question: Is R1 Part 1.8 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

--

DRAFT NERC Reliability Standard Audit Worksheet

Compliance Assessment Approach Specific to CIP-006-6, R1, Part 1.8

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans to log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
	Verify that logs of entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, contains information to identify the individual and date and time of entry.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.9

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.9	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> EACMS; and PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> EACMS; and PCA 	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

Registered Entity Response (Required):

Question: Is R1 Part 1.9 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

DRAFT NERC Reliability Standard Audit Worksheet

Compliance Assessment Approach Specific to CIP-006-6, R1, Part 1.9

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more physical security plans to retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.
	Verify that physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter are retained for at least ninety calendar days.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R1 Part 1.10

CIP-006-6 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.10	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ul style="list-style-type: none"> • PCA 	<p>Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.</p> <p>Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:</p> <ul style="list-style-type: none"> • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection. 	<p>An example of evidence may include, but is not limited to, records of the Responsible Entity’s implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.</p>

Registered Entity Response (Required):

Question: Is R1 Part 1.10 applicable to this audit? Yes No

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:

DRAFT NERC Reliability Standard Audit Worksheet

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-006-6, R1, Part 1.10

This section to be completed by the Compliance Enforcement Authority

	<p>Verify the entity has documented one or more physical security plans to restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.</p> <p>Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document one or more of the following:</p> <ul style="list-style-type: none"> • Encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.
	<p>Verify that the Responsible Entity restricts physical access to cabling and other nonprogrammable communication components used for connection between Cyber Assets of Applicable Systems within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.</p> <p>Where physical access restrictions to such cabling and components are not implemented, verify the Responsible Entity has implemented one or more of the following:</p> <ul style="list-style-type: none"> • encryption of data that transits such cabling and components; or

DRAFT NERC Reliability Standard Audit Worksheet

- | | |
|--|---|
| | <ul style="list-style-type: none">• monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or• an equally effective logical protection. |
|--|---|

Auditor Notes:

DRAFT

R2 Supporting Evidence and Documentation

- R2.** Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]
- M2.** Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-006-6 Table R2 – Visitor Control 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. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

Registered Entity Response (Required):

Question: Is R2 Part 2.1 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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-006-6, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more visitor control programs to require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.
	Verify that the Responsible Entity has implemented a program for continuous escort of individuals who are provided access but are not authorized for unescorted physical access within each Physical Security Perimeter, except during CIP Exceptional Circumstances.
	If the entity has experienced an exception for CIP Exceptional Circumstances, verify the entity has adhered to any applicable cyber security policies.

Auditor Notes:

DRAFT NERC Reliability Standard Audit Worksheet

R2 Part 2.2

CIP-006-6 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> EACMS; and PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> EACMS; and PCA 	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

Registered Entity Response (Required):

Question: Is R2 Part 2.2 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

DRAFT NERC Reliability Standard Audit Worksheet

Compliance Assessment Approach Specific to CIP-006-6 R2 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more visitor control programs to require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.
	Verify that the Responsible Entity performs manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.
	If the entity has experienced an exception for CIP Exceptional Circumstances, verify the entity has adhered to any applicable cyber security policies.

Auditor Notes:

DRAFT

DRAFT NERC Reliability Standard Audit Worksheet

R2 Part 2.3

CIP-006-6 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PCA 	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Registered Entity Response (Required):

Question: Is R2 Part 2.3 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

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

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

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

DRAFT NERC Reliability Standard Audit Worksheet

Compliance Assessment Approach Specific to CIP-006-6, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

<input type="checkbox"/>	Verify the entity has documented one or more visitor control programs to retain visitor logs for at least ninety calendar days.
<input type="checkbox"/>	Verify that visitor logs are retained for at least 90 calendar days.

Auditor Notes:

DRAFT

R3 Supporting Evidence and Documentation

- R3.** Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].
- M3.** Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R3 Part 3.1

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	Applicable Systems	Requirements	Measures
3.1	Physical Access Control Systems (PACS) associated with: <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: <ul style="list-style-type: none"> • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity 	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

Registered Entity Response (Required):

Question: Is R3 Part 3.1 applicable to this audit? Yes No

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

Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

DRAFT NERC Reliability Standard Audit Worksheet

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-006-6, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has documented one or more Physical Access Control System maintenance and testing programs for maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.
	Verify that maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter is conducted at least once every 24 calendar months to ensure they function properly.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-006-6 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

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
DRAFT2v0	09/17/2014	CIP RSAW Development Team	Address comments received in response to DRAFT1v0.
DRAFT3v0	12/10/2014	CIP RSAW Development Team	Address comments received in response to DRAFT2v0.
DRAFT4v0	02/06/2015	CIP RSAW Development Team	Address comments from V5R SDT and address comments in response to DRAFT3v0.
DRAFT4v1	03/09/2015	CIP RSAW Development Team	Address comments from V5R SDT meeting on March 3-4, 2015.

DRAFT