NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-006-6 – Cyber Security — Physical Security of BES Cyber Systems

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.

Findings

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

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

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 physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-5 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-006-5 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.

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
Documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-5 Table R1 – Physical Security Plan
Physical Security Perimeter (PSP) diagrams identifying all PSP access points
Evidence that an alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection of unauthorized access to systems identified in R1 Part 1.5 and R1 Part 1.7.
Logs of physical access into Physical Security Perimeters that show retention of logs for at least 90 days and the individual and the date and time of entry into Physical Security Perimeter(s).

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 STD-0XX-x, R1

This section to be completed by the Compliance Enforcement Authority

High Impact BES Cyber Systems	
	Implemented two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters (includes associated EACMS and PCAs). A sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. *FERC Order No. 706, Paragraph 572 supports utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.* *(Part 1.3)*
	Implemented access monitoring controls for each physical access point into a Physical Security Perimeter (includes associated EACMS and PCAs). Alarm systems are systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. The alarm system should provide alarms for a door forced (opened without authorization), door held (industry standard is 15-30 seconds, but no version of CIP-006 has specified a time threshold), and unauthorized access attempts. In the interest of avoiding "nuisance" alarms, the industry standard for unauthorized access attempt alarming is three consecutive attempts by one person (there is no mention of thresholds in any version of CIP-006). *Examples of methods to monitor physical access include:* Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response. Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access. *(Part 1.4)*
	Ensure the entity has a procedure 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 (includes associated EACMS and PCAs). The entity must have a response procedure for detected unauthorized access. This procedure must include provisions to notify individuals responsible for response to unauthorized access within 15 minutes. The individuals responsible for response should be clearly identified in the procedure and may include security staff, facility/entity management, law enforcement, or others with a defined responsibility to respond to detected unauthorized access. This does not require the entity to activate the notification portion of procedure for false alarms. A good procedure will include provisions to assess and confirm any security system alarms.

	(Part 1.5)
	If unauthorized access through a physical access point into a Physical Security Perimeter was detected did the entity issue an alarm or alert within 15 minutes of detection? Security logs (not necessarily access control logs) should contain both the alarm and the response by security personnel with associated times. (Part 1.5)
	Implement access monitoring controls for each physical access control system protecting PACS. Examples of methods to monitor physical access include: Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response. Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access. *(Part 1.6)*
	Ensure the entity has a procedure to issue an alarm or alert in response to detected unauthorized access to PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection. The entity must have a response procedure for detected unauthorized access. This procedure must include provisions to notify individuals responsible for response to unauthorized access within 15 minutes. The individuals responsible for response should be clearly identified in the procedure and may include security staff, facility/entity management, law enforcement, or others with a defined responsibility to respond to detected unauthorized access. This does not require the entity to activate the notification portion of procedure for false alarms. A good procedure will include provisions to assess and confirm any security system alarms. *(Part 1.7)*
	If unauthorized access to PACS was detected did the entity issue an alarm or alert within 15 minutes of detection? *Security logs (not necessarily access control logs) should contain both the alarm and the response by security personnel with associated times.* *(Part 1.7)*
	Ensure the entity has implemented controls to log 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 (includes associated EACMS and PCAs). Methods to log physical access include: Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access. *When testing logging controls, the auditor should ensure the control captures sufficient information to identify the individual and date and time of entry. For example, video logging may be tested by on site tours by calling the individual monitoring the video feed and asking them to answer the color shirt the auditor is wearing or how many fingers the auditor is holding up.*

	(Part 1.8)
	Ensure the entity has retained ninety calendar days of physical access logs of entry into each Physical Security Perimeter (includes associated EACMS and PCAs). *Part 1.9 requires entities to retain ninety calendar days of physical access logs. In order to confirm this, the audit team should review retained logs to ensure the ninety day threshold is met. This may be accomplished by sampling.* *(part 1.9)*
	Ensure the entity has restricted physical access to cabling and other nonprogrammable communication components used within the same Electronic Security Perimeter when such cabling and components are located outside of a Physical Security Perimeter or implemented alternative measures to protect those cabling and components (includes associated PCAs). Part 1.10 intends to protect cabling and non-programmable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-3 from Pacificorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through equally effective logical protections (such as data encryption or circuit monitoring). Examples of non-programmable components include unmanaged switches, hubs, patch panels, media converters, port savers, couplers, etc. *(Part 1.10)*
	In the event access cannot be restricted to cabling or other nonprogrammable communication components used within the same Electronic Security Perimeter when such cabling and components are located outside of a Physical Security Perimeter, ensure the entity has implemented alternative measures of protection (includes associated PCAs). *Alternative measures of protection may include data encryption or circuit monitoring.* *(Part 1.10)*
Medium Impact BES Cyber Systems with External Routable Connectivity	
	Implemented at least one physical access control to allow unescorted physical access into each Physical Security Perimeter (includes associated EACMS and PCAs). Methods of physical access control include: Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter. The physical access control should effectively deny access to personnel without authorized unescorted access. *(Part 1.2)*
	Implemented access monitoring controls for each physical access point into a Physical Security Perimeter

	(includes associated EACMS and PCAs). *Alarm systems are systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. The alarm system should provide alarms for a door forced (opened without authorization), door held (industry standard is 15-30 seconds, but no version of CIP-006 has specified a time threshold), and unauthorized access attempts. In the interest of avoiding "nuisance" alarms, the industry standard for unauthorized access attempt alarming is three consecutive attempts by one person (there is no mention of thresholds in any version of CIP-006).* *Examples of methods to monitor physical access include:* Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response. Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access. *(Part 1.4)*
	Ensure the entity has a procedure 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 (includes associated EACMS and PCAs). The entity must have a response procedure for detected unauthorized access. This procedure must include provisions to notify individuals responsible for response to unauthorized access within 15 minutes. The individuals responsible for response should be clearly identified in the procedure and may include security staff, facility/entity management, law enforcement, or others with a defined responsibility to respond to detected unauthorized access. This does not require the entity to activate the notification portion of procedure for false alarms. A good procedure will include provisions to assess and confirm any security system alarms. *(Part 1.5)*
	If unauthorized access through a physical access point into a Physical Security Perimeter was detected did the entity issue an alarm or alert within 15 minutes of detection? The entity must have a response procedure for detected unauthorized access. This procedure must include provisions to notify individuals responsible for response to unauthorized access within 15 minutes. The individuals responsible for response should be clearly identified in the procedure and may include security staff, facility/entity management, law enforcement, or others with a defined responsibility to respond to detected unauthorized access. This does not require the entity to activate the notification portion of procedure for false alarms. A good procedure will include provisions to assess and confirm any security system alarms. *(Part 1.5)*
	Implement access monitoring controls for each physical access control system protecting PACS. *Examples of methods to monitor physical access include:* Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response. Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access. *(Part 1.6)*

	Ensure the entity has a procedure to issue an alarm or alert in response to detected unauthorized access to PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection. The entity must have a response procedure for detected unauthorized access. This procedure must include provisions to notify individuals responsible for response to unauthorized access within 15 minutes. The individuals responsible for response should be clearly identified in the procedure and may include security staff, facility/entity management, law enforcement, or others with a defined responsibility to respond to detected unauthorized access. This does not require the entity to activate the notification portion of procedure for false alarms. A good procedure will include provisions to assess and confirm any security system alarms. *(Part 1.7)*
	If unauthorized access to PACS was detected did the entity issue an alarm or alert within 15 minutes of detection? Security logs (not necessarily access control logs) should contain both the alarm and the response by security personnel with associated times. *(Part 1.7)*
	Ensure the entity has implemented controls to log 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 (includes associated EACMS and PCAs). Methods to log physical access include: Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method. Video Recording: Electronic capture of video images of sufficient quality to determine identity. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access. *When testing logging controls, the auditor should ensure the control captures sufficient information to identify the individual and date and time of entry. For example, video logging may be tested by on site tours by calling the individual monitoring the video feed and asking them to answer the color shirt the auditor is wearing or how many fingers the auditor is holding up.* *(Part 1.8)*
	Ensure the entity has retained ninety calendar days of physical access logs of entry into each Physical Security Perimeter (includes associated EACMS and PCAs). Part 1.9 requires entities to retain ninety calendar days of physical access logs. In order to confirm this, the audit team should review retained logs to ensure the ninety day threshold is met. This may be accomplished by sampling. *(part 1.9)*
Medium Impact BES Cyber Systems at Control Centers	
	Ensure the entity has restricted physical access to cabling and other nonprogrammable communication components used within the same Electronic Security Perimeter when such cabling and components are located outside of a Physical Security Perimeter or implemented alternative measures to protect those cabling and components (includes associated PCAs). Part 1.10 intends to protect cabling and non-programmable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-3 from Pacificorp,

	must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through equally effective logical protections (such as data encryption or circuit monitoring). Examples of non-programmable components include unmanaged switches, hubs, patch panels, media converters, port savers, couplers, etc. *(Part 1.10)*
	In the event access cannot be restricted to cabling or other nonprogrammable communication components used within the same Electronic Security Perimeter when such cabling and components are located outside of a Physical Security Perimeter, ensure the entity has implemented alternative measures of protection (includes associated PCAs). Alternative measures of protection may include data encryption or circuit monitoring. *(Part 1.10)*
Medium BES Cyber Systems without External Routable Connectivity	
	Ensure the entity implemented operational and/or procedural controls to restrict access physical access (includes associated EACMS and PCAs). Examples of operational or procedural controls may include a defined boundary with physical access controls such as locks or card-controlled doors. Procedural controls may include signage restricting access to authorized personnel or locating assets in a restricted area. *(Part 1.1)*
Note to Auditor: Each Part of R1 requires both documentation review and proof of performance. Proof of performance should be conducted through direct observation (site tours). Site tours may be conducted on a sampled basis.	

Auditor Notes:

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-006-5 Table R2 – Visitor Control Program.

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
Documented visitor control program that collectively includes all of the applicable requirement parts in CIP-006-5 Table R2 – Visitor Control Program
Logs of physical access by visitors in and out of Physical Security Perimeters that show retention of logs for at least 90 days and the individual and date and time of entry to and exit from Physical Security Perimeters.

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 STD-006-6, R2

This section to be completed by the Compliance Enforcement Authority

High Impact BES Cyber Systems and their associated EACMS and PCA

	Ensure the entity has a documented a visitor program. (Requirement R2)
	Ensure the visitor control program requires continuous escorting of visitors within each Physical Security Perimeter. A point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor. *(Part 2.1)*
	Ensure the visitor control program requires logging of visitor entry into and exit from Physical Security Perimeter(s). The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit. *(Part 2.2)*
	Review visitor logs for proof of performance. The auditor should review visitor logs to ensure visitors are logged with sufficient detail to identify the visitor and their point of contact at the entity. *(Part 2.2)*
	Ensure visitor logs include 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. The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit. *(Part 2.2)*
	Ensure visitor logs are maintained for at least ninety calendar days. Part 2.3 requires entities to retain ninety calendar days of visitor logs. In order to confirm this, the audit team should review retained logs to ensure the ninety day threshold is met. This may be accomplished by sampling. *(Part 2.3)*
Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS and PCA	
	Ensure the entity has a documented a visitor program. (Requirement R2)
	Ensure the visitor control program requires continuous escorting of visitors within each Physical Security Perimeter. A point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor. *(Part 2.1)*
	Ensure the visitor control program requires logging of visitor entry into and exit from Physical Security Perimeter(s). The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit. *(Part 2.2)*
	Review visitor logs for proof of performance. The auditor should review visitor logs to ensure visitors

	are logged with sufficient detail to identify the visitor and their point of contact at the entity. (Part 2.2)
	Ensure visitor logs include 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. The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit. *(Part 2.2)*
	Ensure visitor logs are maintained for at least ninety calendar days. Part 2.3 requires entities to retain ninety calendar days of visitor logs. In order to confirm this, the audit team should review retained logs to ensure the ninety day threshold is met. This may be accomplished by sampling. (Part 2.3)
Note to Auditor: At a minimum visitor logs should be requested for the final week of the audit period and the week 90 days prior to the end of the audit period. Implementation of visitor logs should also be confirmed on site tours.	

Auditor Notes:

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-006-5 Table R3 – Maintenance and Testing

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-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Registered Entity Response (Required):

Compliance Narrative:

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

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
Documented Physical Access Control System maintenance and testing program(s)
Documentation demonstrating testing and maintenance performed on each applicable device or system at least once every 24 calendar months.

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 STD-006-6, R3

This section to be completed by the Compliance Enforcement Authority

PACS Associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems with External Routable Connectivity	
	Review maintenance and testing program for PACS and locally mounted hardware or devices at the PSP. 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. This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems. *(Requirement R3)*
	Review evidence to ensure maintenance and testing occurred at least once every 24 months for PACS and locally mounted hardware or devices at the PSP. Evidence should demonstrate that this testing was done. Evidence may include 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. *(Part 3.1)*
Locally mounted hardware or devices at the Physical Security Perimeter associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems with External Routable Connectivity	
	Review maintenance and testing process for PACS and locally mounted hardware or devices at the PSP. 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. This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems. *(Requirement R3)*
	Review evidence to ensure maintenance and testing occurred at least once every 24 months for PACS and locally mounted hardware or devices at the PSP. Evidence should demonstrate that this testing was done. Evidence may include 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. *(Part 3.1)*
Note to Auditor: In the event an entity has a large number of devices at the PSP perimeter, NERC sampling methodology may be used.	

Auditor Notes:

Reliability Standard

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

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

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

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

Sampling Methodology

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

Regulatory Language

See FERC Order 706
See FERC Order 791

Selected Glossary Terms

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

Revision History for RSAW

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

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