
Reliability & Security
Workshop
WECC
March 17–18, 2026
San Diego, California

CIP-006-6 R1&R3 Audit Approach

Joshua Rowe, PSP
Manager, Entity Monitoring

Electric Reliability & Security for the West

March 18, 2026

Agenda

- Requirement Overview
- Audit Approach
- Audit Questions
- PACS Testing
- PACS Maintenance
- Audit Observations
- Questions/Discussion

Requirement Overview

CIP-006-6 Requirement 1

Physical security plans addressing operational or procedural controls to restrict physical access, access controls, monitoring, alerting, and logging

Applicable Systems

High Impact BES Cyber Systems

- EACMS
- PACS
- PCA
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity

- EACMS
- PACS
- PCA
- PACS

Physical Access Control Systems (PACS)

CIP-006-6 Requirement 3

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

Applicable Systems

Physical Access Control Systems (PACS) and locally mounted hardware or devices associated with:

- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems with External Routable Connectivity

NERC Definition

Physical Security Perimeter

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

NERC Definition

Physical Access Control System

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

What is Locally Mounted Hardware?

- Motion sensors
- Electronic lock control mechanisms (door strikes)
- Badge readers
- Audible sounders
- Visual siren
- CCTV

Audit Approach

Initial Evidence Review

- Assess and validate the evidence submission to ensure it is sufficient and appropriate.
  - Is the evidence in an acceptable format?
  - Is the evidence applicable to the Reliability Standard and Requirement?
  - Does the evidence match the sample requests?
  - Does the evidence cover the applicable audit period?
- Review Compliance Narrative
  - Did the entity provide a detailed compliance narrative?
  - Did the entity provide all the files referenced in the narrative?
  - Does the evidence support the compliance narrative?

Gathering Evidence (R1- Level 1)

Evidence Request Tool (v10)

CIP-006-6-R1-L1-01	CIP-006-6	R1	Provide each documented physical security plan(s) that collectively includes all the applicable requirement parts in CIP-006 R1.
CIP-006-6-R1-L1-02	CIP-006-6	R1	Provide details of PACS network connectivity, such as schematics, diagrams, or other documentation, to control panels at applicable physical access points (e.g., PACS servers, workstations, database units, and/or control panels at physical access points).
CIP-006-6-R1-L1-03	CIP-006-6	R1 Part 1.5 R1 Part 1.7	Provide each documented Cyber Security Incident response plan(s) that identify personnel who will receive an alarm or alert in response to detected unauthorized physical access into a Physical Security Perimeter (PSP).
CIP-006-6-R1-L1-04	CIP-006-6	R1 Part 1.10	For all high impact BES Cyber Systems, and associated PCA, and/or all medium impact BES Cyber Systems at Control Centers, and associated PCA, provide evidence of 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 for those instances when cabling and components used for connection between applicable Cyber Assets within the same ESP are located outside of a PSP.

Gathering Evidence (R1- Level 2)

Evidence Request Tool (v10)

CIP-006-6-R1-L2-01	CIP-006-6	R1 Part 1.1	For each BES Cyber System in Index Sample Set CA-L2-07, provide evidence that operational or procedural controls have been implemented to restrict access to each component Cyber Asset of the BES Cyber System.
CIP-006-6-R1-L2-02	CIP-006-6	R1 Part 1.1	For each Physical Access Control System in Index Sample Set CA-L2-08, provide evidence that operational or procedural controls have been implemented to restrict access.
CIP-006-6-R1-L2-03	CIP-006-6	R1 Part 1.2	For each Physical Security Perimeter in Index Sample Set PSP-L2-01, provide evidence identifying each physical access point and the physical access control(s) used.
CIP-006-6-R1-L2-04	CIP-006-6	R1 Part 1.3	For each Physical Security Perimeter in Index Sample Set PSP-L2-02, provide evidence identifying each physical access point and the physical access control(s) used or that an approved TFE covers this circumstance.
CIP-006-6-R1-L2-05	CIP-006-6	R1 Part 1.2 R1 Part 1.3	For each Physical Security Perimeter in Index Sample Sets PSP-L2-03, if a physical keyway is an alternate method of access control, provide evidence of physical hard-key management, inventory, and use.
CIP-006-6-R1-L2-06	CIP-006-6	R1 Part 1.4	For each physical access point in Index Sample Set PSP-L2-03, provide evidence of monitoring for unauthorized physical access through the physical access point into the Physical Security Perimeter for the dates in SS-DATE-01.

Gathering Evidence (R1- Level 2 Continued)

Evidence Request Tool (v10)

CIP-006-6-R1-L2-07	CIP-006-6	R1 Part 1.5	For each physical access point in Index Sample Set PSP-L2-03, provide evidence of an alarm or alert was generated in response to detected unauthorized physical access into a Physical Security Perimeter. Include evidence of personnel in the Cyber Security Incident response plan were notified within 15 minutes of detection for the dates in SS-DATE-01. If none were generated during SS-DATE-01, provide evidence of the capability to generate an alarm or alert to the personnel in the Cyber Security Incident response plan.
CIP-006-6-R1-L2-08	CIP-006-6	R1 Part 1.6	For each Physical Access Control System in Index Sample Set CA-L2-08, provide evidence of monitoring for unauthorized physical access to the PACS for the dates in SS-DATE-01.
CIP-006-6-R1-L2-09	CIP-006-6	R1 Part 1.7	For each Physical Access Control System in Index Sample Set CA-L2-08, provide evidence an alarm or alert was generated in response to detected unauthorized physical access to the PACS. Include evidence personnel in the Cyber Security Incident response plan were notified within 15 minutes of detection for the dates in SS-DATE-01. If none were generated during SS-DATE-01, provide evidence of the capability to generate an alarm or alert to the personnel in the Cyber Security Incident response plan.
CIP-006-6-R1-L2-10	CIP-006-6	R1 Part 1.8 R1 Part 1.9	For each Physical Security Perimeter in Index Sample Sets PSP-L2-03, provide logs of individual physical access, including information to identify the individual and date and time of entry for the dates in SS-DATE-01.

Gathering Evidence (R3- Levels 1&2)

Evidence Request Tool (v10)

CIP-006-6-R3-L1-01	CIP-006-6	R3	Provide each documented PACS maintenance and testing program(s) that collectively includes each of the applicable requirement parts in CIP-006 R3.

CIP-006-6-R3-L2-01	CIP-006-6	R3 Part 3.1	For each Physical Access Control System in Index Sample Set CA-L2-08, provide evidence of maintenance and testing of each PACS and locally mounted hardware or devices at the Physical Security Perimeter occurred at least once every 24 calendar months during the audit period.
CIP-006-6-R3-L2-02	CIP-006-6	R3 Part 3.1	For each Physical Security Perimeter in Index Sample Sets PSP-L2-03, provide evidence of maintenance and testing of each PACS and locally mounted hardware or devices at the Physical Security Perimeter occurred at least once every 24 calendar months during the audit period.

Sampling considerations should include a variety of:

- Workstations
- Controllers (PACS Panel)
- Servers

Audit Questions

Common Audit Questions (R1)

- Is the physical security plan a stand-alone document, or are supporting policies/processes/procedures referenced?
- Did the entity provide PSP diagrams?
- Are PACS located within a PSP or a separate secured zone?
- Does the plan define operational or procedural controls to restrict physical access?
- What are operational and procedural controls?
- What physical access controls are being used?
- Is there a single perimeter or layered?
- How does the entity verify only authorized individuals are allowed access?

Common Audit Questions (R1 Continued)

- Was a TFE filed for any Cyber Assets associated with the sampled PSP?
- If physical keys are used, does the entity have a documented hard key management procedure?
- What controls does the entity have for monitoring unauthorized access?
- Does the entity have a security operations center?
- Are the personnel monitoring for unauthorized access also part of the CSIRT?
- Does the entity retain logs for the minimum amount of time (90 days) or longer?
- How is access restricted to PACS located outside of a PSP?
- What methods does the entity have for issuing an alarm or alert in response to detected unauthorized access?

Common Audit Questions (R1 Continued)

- Are there both primary and secondary methods for alarming/alerting?
- Who are the personnel in the CSIRT and how are they notified?
- Is a human assessment being performed?
- If an assessment is being performed, how does the entity determine detected unauthorized access?
- How is logging being performed? Automated or manual?
- What are the procedures for manual logging?
- How are individuals identified?
- Is the date and time of entry logged?
- Does the entity retain logs for the minimum amount of time (90 days) or longer?
- How is access to physical cabling and communication components restricted?

Common Audit Questions (R3)

- Is the program a stand-alone document or embedded into a physical security plan?
- Does the plan identify the requirement to perform maintenance and testing at least once every 24 calendar months?
- Did the entity identify roles and responsibilities for personnel assigned maintenance and testing duties?
- Does the entity perform maintenance and testing in house or is it contracted to a third-party vendor?
- If a third-party vendor is used, does the contract support the required tests?
- Does the entity maintain a list of all PACS and peripheral components by serial number?

Common Audit Questions (R3 Continued)

- Does the entity maintain diagrams depicting the location of all PACS and peripheral devices?
- Do the lists and diagrams account for all PACS and peripheral devices?
- Does the entity use a maintenance and testing checklist?

PACS Testing

Testing Activity

- Did the entity identify the appropriate tests?
  - Valid Entry (Authorized Badge)
  - Invalid Entry (Unauthorized Badge)
  - Valid Entry (Authorized Badge + PIN)
  - Invalid Entry (Authorized Badge wrong PIN)
  - Door Held Open
  - Door Forced Open
    - Physical Hard Key
    - Request to exit not used
    - Rare earth magnet

Testing Activity

- Anti-tailgate
- Anti-pass back
- Audible sounder
- Visual siren
- Intrusion detection sensors (PIR, IR, vibration, acoustic, etc.)
- Tamper switches
- Duress button
- Power failure
- Communication failure (network failure)
- Fire alarm testing (fail open/fail safe)

Testing Activity

- Workstation login
  - Valid credentials
  - Invalid credentials
- Workstation arm/disarm (doors/sensors)
- Workstation lock/unlock (doors)
- Uncommon tests
  - Mobile phone (NFC) badge
  - Biometric (fingerprint/eye pattern/voice)
  - AI-phone
  - American Disabilities Act (ADA doors/gates)

PACS Maintenance

Maintenance Activity

- Did the entity identify the appropriate maintenance items?
  - Visual inspection
  - Rating/output of power supply
  - Rating/output of battery back-up
  - Lubricate moving parts (hinges, door strikes, etc.)
  - Verify communication connections are secure
  - Verify panels are free of dust/debris

Controls

- What records are archived after maintenance and testing?
  - Checklist
  - Diagrams
  - Alarm logs
  - Attestations
- If a test failure occurs, what are the procedures to repair or replace devices?
- If an entity employee discovers a failed or damaged PACS or locally mounted hardware device, do they know how to report it?
- Does the entity have a plan/procedure for after-hours/emergency response to repair or replace a failed device?
- If a new device is installed, what are the procedures for updating lists, diagrams, and testing checklists?

Audit Observations

Observations (R1)

- Logs contain first or last name only
- Manual logs are illegible
- System Operator’s monitoring PACS alarms as secondary responsibility
- Not documenting hard key management program
- Poor documentation of 2FA; Ensuring authentication occurs prior to access
- Enhancing capability for real-time remote alarm assessment for 1.4/1.6
- Poorly documented key management program
- Poorly documented components of physical security plan
- Poorly documented roles and responsibilities in PSP or CSIRP

Observations (R3)

- Minimal testing (DFO, DHO, valid badge, etc.)
- Incomplete list of PACS or locally mounted hardware
- Alarm logs not retained with PACS testing checklists
- Peripheral devices (door sounders, visual sounders, duress buttons) not tested

Questions/Discussion


Reliability & Security Workshop
WECC
Take our survey!

WICF Meeting

Thursday, March 19

Breakfast 7:30–8:30 a.m. PDT

Meeting 8:30 a.m.–12:15 p.m. PDT

Lunch 12:15 –1:45 p.m. PDT

Meeting 1:45–3:25 p.m. PDT

ELECTRIC RELIABILITY & SECURITY FOR THE WEST

ENGAGE WITH WECC

WECC

engage@wecc.org

www.wecc.org | 801-582-0353

155 N 400 W, Salt Lake City, Utah 84103, USA