Electric Reliability and Security for the West

Internal Controls
Failure Points and Guidance Questions
CIP-006-6 R1

Security Objective

The organization monitors physical access to the protected systems and to organization-defined spaces containing one or more components of the protected systems.

The organization also—

- Develops, documents, and disseminates a physical and protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- Develops, documents, and disseminates procedures to help implement the physical protection policy and associated physical and protection controls; and
- Reviews and updates the current physical protection policy and procedures.

NIST Special Publication 800-53 (Rev. 4) PE-1, 2, 3, 6(4)

WECC Intent

The potential failure points and guidance questions give direction to registered entities for assessment of risk, while designing internal controls specific to NERC Reliability Standards and Requirements. The Registered Entity may use this document as a starting point in determining entity risk. It is not WECC's intent to establish a standard or baseline for entity risk assessment or controls design.

Note: *Guidance questions help an entity understand and document its controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance at audit.*

**Please send feedback to ICE@WECC.org with suggestions on potential failure points and guidance questions.*

Potential Failure Points & Guidance Questions

CIP-006-6 R1

Potential Failure Point (R1): Failure to develop plans that define and apply operational or procedural controls to restrict physical access.

1. Do you have a review process to ensure all topics are addressed?
2. How do you ensure the documented physical security plans are used?
   a. Are there any controls to track the use of the plans?

   b. How do you determine when the security plans need to be updated?
3. Do you have a process to evaluate whether operational or procedural controls effectively mitigate the risk of unauthorized physical access?
4. Describe any training you use that covers operational controls to restrict physical access to BES Cyber Systems.
5. How do you ensure that the documented physical security plans in effect?
   a. How do you track the execution of the plans?
   b. How do you determine when the security plans need to be updated?
6. How do you ensure all personnel are made aware of the operational and procedural controls to restrict physical access?

Potential Failure Point (R1): Failure to develop a complete list of assets that require a process to restrict physical access

1. How do you ensure personnel are aware of all assets that need controls to restrict physical access?
2. Describe your method for identifying Physical Access Control Systems (PACS) assets.

Potential Failure Point (Part 1.2): Failure to define each Physical Security Perimeter (PSP) in physical security plan.

1. How do you verify all PSPs are included in plan(s)?
2. How does your plan address dual-use spaces?
3. How does your plan(s) address changes in use of space that may trigger a classification?

Potential Failure Point (Part 1.2): Failure to define authorization criterion or procedures.

1. How do you determine who is authorized to have unescorted physical access into the PSP?
2. Has you established a process to inform individuals whether they do or do not have authorized unescorted physical access to a PSP?

Potential Failure Point (Part 1.2): Failure to define a physical access control.

1. Do you have a back-up method for controlling physical access?
   a. How is it documented?
2. Are employees aware of the back-up method in the event of a failure to the primary method?

Potential Failure Point (Part 1.3): Failure to define physical access controls to be used per access location.

1. Do you have a documented process to define the two or more different physical access controls?
2. Do you have a back-up method for controlling physical access?
   a. How is it documented?
3. Are employees aware of the back-up method in the event of a failure to one or more of the primary access controls?

4. How does your back-up method ensure each person meets the two-factor authentication requirement of "something you have, something you are, or something you know" before entering the PSP?

Potential Failure Point (Part 1.4): Failure to define methods for monitoring for unauthorized access.

1. How do you verify all PSPs are actively monitored by a PACS or another method?
2. How do you determine methods that can be used to monitor for unauthorized access through a physical access point into the PSP?
   a. How do you evaluate those controls and methods if the environment changes?
   b. Do you have a secondary method to monitor for unauthorized access in the event of a failure or outage to the primary method?

Potential Failure Point (Part 1.5): Failure to define alarm or alert criterion for detected unauthorized access.

1. How does the documented physical security plan describe how PACS issue alarm or alert in response to detected unauthorized access?
2. How does the documented physical security plan describe how alarm or alerts are issued in response to detected unauthorized access in the event of PACS failure?

Potential Failure Point (Part 1.5): Failure to develop incident response procedures for alarms or alerts in the plan.

1. How do you document response procedures?
2. How do you ensure response personnel are trained to respond to incidents?
3. How do you document responses to all alarm activity?

Potential Failure Point (Part 1.5, 1.7): Failure to clearly define or communicate start and end times and dates used to establish periods for incident response.

1. How does the plan outline actions taken to ensure alarms or alerts will be responded to within 15 minutes of detection?
2. How do you document alarm acknowledgement, response, and notification within 15 minutes of detection?

Potential Failure Point (Part 1.5): Failure to identify personnel required to respond in plan.

1. How do you define roles in your plan(s)?
2. Does each person understand their role in the plan?
3. Do the Cyber Security Incident Response plan and physical security plan complement each other for incident response?

Potential Failure Point (Part 1.6): Failure to define alarm or alert criterion for detected unauthorized access.

1. Do you have a process to establish controls that can be used to detect unauthorized access through a physical access point into the PACS?
2. How do you determine methods that can be used to monitor for unauthorized access to a PACS?
3. How do you validate all PACS asset monitoring with a known list of PACS assets?

Potential Failure Point (Part 1.6): Failure to define monitoring methods.

1. How do you determine methods that can be used to monitor for unauthorized access through a physical access point into the PACS?
    a. How do you evaluate those controls and methods if the environment changes?
    b. How do you designate a secondary method to monitor for unauthorized access in case of a failure or outage to the primary method?

Potential Failure Point (Part 1.7): Failure to define alarm or alert criterion for detected unauthorized access.

1. How does the documented physical security plan describe how PACS issue alarm or alert in response to detected unauthorized access?
2. How does the documented physical security plan describe how alarm or alerts are issued in response to detected unauthorized access in the event of PACS failure?

Potential Failure Point (Part 1.7): Failure to develop incident response procedures for alarms or alerts in plan.

1. How do you document the responses?
2. How do you ensure response personnel are trained to respond to incidents?
3. How do you document responses to all alarm activity?

Potential Failure Point (Part 1.7): Failure to clearly define or communicate start and end times and dates used to establish periods for incident response.

1. How does the plan outline actions taken to ensure alarms or alerts will be responded to within 15 minutes of detection?
2. How do you document alarm acknowledgement, response, and notification within 15 minutes of detection?

Potential Failure Point (Part 1.7): Failure to identify personnel required to respond in plan.

1. How do you define roles in your plan(s)?
2. How do you ensure each person understands their role in the plan?
3. How do your Cyber Security Incident Response plan and physical security plan complement each other for incident response?

Potential Failure Point (Part 1.8): Failure to define logging parameters or procedures that record required details of the CIP-006-6 R1.8 requirement.

1. If applicable, how do you communicate procedures to the personnel responsible for controlling entry?
    a. How do you ensure all personnel have been trained?
2. In automated systems, how do you verify logging parameters?
3. How do you accomplish manual logging in case of an automated logging failure?
4. How do you ensure you have given clearly documented, manual logging procedures?
5. How do you verify manual logging for all personnel at each PSP?

Potential Failure Point (Part 1.9): Failure to define logging requirements or procedures that specify retention of records as required by CIP-006-6 R1.9.

1. How do you retain automated logs?
    a. How do you retain electronic logs?
2. Where logs are recorded manually by personnel who control entry, what is your process to ensure logs are retained?
    a. How do you ensure the logs are dated and timed?
3. How do you consolidate manual logs at multiple locations?

Potential Failure Point (Part 1.10): Failure to document cable paths.

1. Does your cabling documentation give enough detail to determine whether protective measures are required?

Potential Failure Point (Part 1.10): Failure to define nonprogrammable communication components.

1. How do you define nonprogrammable communications components?

Potential Failure Point (Part 1.10): Failure to define methods that restrict physical access.

1. Where applicable, how do you define methods that restrict physical access?

Potential Failure Point (Part 1.10): Failure to define criterion for not implementing physical access restrictions.

1. Where applicable, how do you determine if physical access restrictions are possible or feasible?
    a. Is there a review process of determinations?

Potential Failure Point (Part 1.10): Failure to define methods of encryption.

1. Where applicable, how do you determine methods of encryption?

Potential Failure Point (Part 1.10): Failure to define methods to detect communication failures.

1. Where applicable, how do you establish methods to determine communication failures?

Potential Failure Point (Part 1.10): Failure to define alarm or alert criterion for communication failures.

1. Where applicable, how do you define alarm or alert criterion for communication failures?

Potential Failure Point (Part 1.10): Failure to develop incident response procedures for alarms or alerts in the plan.

1. How does your physical security plan outline incident response for communication failures?

Potential Failure Point (Part 1.10): Failure to identify personnel required to respond in plan.

1. How do you define roles in your plan(s)?
2. How do you ensure each person understands their role in the plan?
3. How do your Cyber Security Incident Response plan and physical security plan complement each other for incident response?

Potential Failure Point (Part 1.10): Failure to define allowable logical protections.

1. Where applicable, how do you define allowable logical protections?