Electric Reliability and Security for the West

Internal Controls
Failure Points/Guidance Questions
CIP-004-6 R1

Security Objective

- Develop, document, and disseminate a security awareness and training program to organization-defined personnel or roles. The program must address—
  - Purpose,
  - Scope,
  - Roles,
  - Responsibilities,
  - Management commitment,
  - Coordination among organizational entities, and
  - Required compliance.
- Develop procedures to put in place the security awareness and training program and associated security awareness and training controls, reviews, and updates.

NIST Special Publication 800-53 (Rev. 4) AT-1

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

Potential Failure Point: Failure to develop a procedure on methods that provide security awareness.

1. How do you ensure awareness methods are performed at least once each quarter?
2. Do you have a defined process to ensure all personnel, who have authorized electronic or unescorted physical access to BES Cyber Systems, are included in cybersecurity awareness communications?

   a. Do you have a process to ensure that security awareness communications have been received?
3. Do you have a process to determine the effectiveness of the security awareness program?
   a. How do you ensure continuous improvement of the security awareness program based on changing cybersecurity risks?

Potential Failure Point: Failure to define cybersecurity practices to be followed.

1. How do you define security (or associated) practices?

Potential Failure Point: Failure to develop a procedure on how to identify personnel who have authorized electronic or unescorted physical access to BES Cyber Systems.

1. Do you have a defined process to determine which personnel should be included in security awareness communications?
2. How do you ensure that personnel have received security awareness communications?