Electric Reliability and Security for the West

Internal Controls
Failure Points and Guidance Questions
CIP-011-2 R1, R2

Security Objective

- Development of programs to identify, protect, and handle organization-defined types of digital and non-digital information.
- Prevent unauthorized access to BES Cyber System Information.
- Prevent the unauthorized retrieval of organization-defined information on media before disposal, release from organizational control, or release for reuse using organization-defined sanitization techniques and procedures.
- Use sanitizing mechanisms with the strength and integrity equal to the security category or classification of the information.

NIST Special Publication 800-53 (Rev. 4) MP-1, MP-6

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-011-2 R1

Potential Failure Point: Failure to develop a policy to prevent unauthorized access to BES Cyber System Information.

1. How do you enforce this policy?
2. How have you communicated the requirement to prevent unauthorized access?

Potential Failure Point (Part 1.1): Failure to develop methods to identify BCSI.

1. What methodology do you use to identify BCSI?

   a. How do you document these inventories or repositories?
      i. Is there a periodic review of inventories?
      ii. How do you document the review?
2. How do you handle data class indicators on information (e.g., labels or classification) that identify BES Cyber System Information?
   a. Are classifications those designated in the entity's information protection program?

Potential Failure Point (Part 1.2): Failure to develop a process to document methods for storage, transmission, or use of BCSI.

1. Does procedure cover all forms of storage, transmission, and usage?
   a. Does it include forms of removable media?

Potential Failure Point (Part 1.2): Failure to develop a procedure that outlines how protections and handling is to occur.

1. Do the protections and handling address both electronic and physical forms of information?
2. Does the procedure address access removal in all forms?
3. How do you train employees on procedure(s)?
4. How do you enforce the procedure?

CIP-011-2 R2

Potential Failure Point (R2): Failure to develop a policy to prevent unauthorized access to BES Cyber System Information.

1. How do you enforce this policy?
2. How do you communicate the requirement to prevent unauthorized retrieval?

Potential Failure Point (R2): Failure to develop and use methods to prevent unauthorized retrieval of BES Cyber System Information.

1. Do you use automated or manual processes to prevent unauthorized retrieval?
2. For manual processes used to prevent unauthorized retrieval, how do you monitor the process to ensure it is executed properly?
   a. How do you ensure that the responsible individual(s) know the manual process(es)?
   b. How would you become aware of a failure?

Potential Failure Point (R2): Failure to develop a process to determine all assets containing BCSI.

1. How do you ensure that all Cyber Assets containing BES Cyber System Information are identified?

Potential Failure Point (R2): Failure to develop a process to track asset before removal of protected information.

1. How do you provide guidance on asset disposal?
2. How do you provide guidance on asset reuse?
   a. What measures do you take to protect asset until process is complete?
   b. Is there a chain-of-custody procedure to track asset until process is complete?
3. Does your process address all applicable assets?
4. How do you ensure that the actions taken are recorded correctly?
   a. Is there a review or verification process following sanitation efforts?