Electric Reliability and Security for the West

Self-Certification Summary
CIP-003-8 – Security Management Controls
September 2024

Overview

As part of the risk-based Compliance Monitoring and Enforcement Program (CMEP), WECC is conducting a Self-Certification on security management controls (CIP-003-8 R2, Attachment 1, Sections 2, 3, and 5). The Self-Certification includes the questions below for selected registered entities.[1]

Note: Responses to these questions should be brief. They should be entered in the corresponding text boxes provided in the Self-Certification request in Align and not via the Secure Evidence Locker (SEL).

Questions

CIP-003-8 R2

Internal Controls

1. Are any NERC regulatory compliance programs managed by a party other than your entity? If yes, please identify which NERC Reliability Standard Requirement(s) are managed by the party.
2. Does your entity or third-party conduct an internal audit or mock audit of your NERC regulatory compliance programs?

Critical Infrastructure Protection (CIP)

3. Does your entity own or operate any Bulk Electric System (BES) assets containing a BES Cyber System (BCS)? If yes, please provide the number of BCS and their associated impact rating (high, medium, or low). If no, briefly explain the reason(s) for no BCS, skip questions 4 through 15, and select a compliance response for this requirement.
4. How frequently are cyber and physical security policies, procedures, and plans reviewed and when were the last significant updates made?

Attachment 1, Section 2 – Physical Security Controls

5. What methods or tools are used to control physical access, based on need for the following: (a) The asset or the locations of the low impact BES Cyber System(s) within the asset; and (b) Any Cyber Asset(s) that provide electronic access control(s).
6. Does your entity conduct a risk assessment or threat evaluation to determine the points in most need of protection?

[1] These self-certifications are marked SCwQ in Align for tracking purposes.

7. Do you have a hard key management procedure and/or a process for revoking physical access?
8. Does your entity have dedicated personnel responsible for implementing and overseeing physical security policies, procedures, and measures at your facilities?
9. What types of monitoring systems (e.g., cameras, sensors) are used to oversee physical access points?
10. Do you have any training programs in place for personnel with physical access to facilities with low impact BCS?

Attachment 1, Section 3 – Electronic Access Controls

11. What methods or tools are used to permit only necessary inbound and outbound electronic access for any of the following communications that are: (a) Between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); (b) Using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and (c) Not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).
12. How many external routable connections are there from your asset(s) to non-NERC entities, such as contractors, vendors, or other third parties?

Attachment 1, Section 5 – Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

13. Does your entity manage the use of Transient Cyber Assets (TCA) to connect to BCS? If yes, what methods or tools are used to mitigate the introduction of malicious code and identify if the TCAs are managed in a manner that is on-demand, ongoing, or a combination of both.
14. Does your entity allow the use of TCAs managed by a party other than your entity to connect to a BCS? If yes, what methods or tools are used to mitigate the introduction of malicious code prior to connecting to a BCS, for the TCAs managed by the party?
15. Does your entity allow Removable Media to be connected to a BCS? If yes, what methods or tools are used to detect and mitigate the threat of malicious code?

Compliance Response

Please indicate your response for this requirement. (Compliant, Non-Compliant, Not Applicable, Do Not Own)