ERO Enterprise CMEP Practice Guide:

BES Cyber System Information

April 26, 2019

Background

In support of successful implementation of and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.[3]

Purpose

The purpose of this CMEP Practice Guide is to provide guidance to ERO Enterprise CMEP staff (CMEP staff) when assessing a registered entity's process to authorize access to designated storage locations for BES Cyber System Information (BCSI) pursuant to CIP-004-6 Requirement R4, and any access controls the registered entity implemented as part of its CIP-011-2 Requirement R1 procedure(s). This Practice Guide outlines aspects that CMEP staff should consider in understanding how a registered entity has applied access controls to mitigate the reliability risk associated with accessing BCSI. This risk information can be used to inform CMEP staff's understanding of a registered entity's security posture and commensurate Compliance Oversight (i.e., Compliance Oversight Plan, audit approach, etc.). Compliance determinations are to be made in light of specific facts and circumstances of the individual registered entities and the language of the Requirements.

Access and Authorization to BCSI

Responsible Entities implement access controls, including access authorization, to meet their obligations under CIP-004-6 and CIP-011-2. As required in CIP-004-6 Requirement R4, Part 4.1.3, Responsible Entities must have a process to authorize, based on need, access to designated storage locations, whether physical or electronic, for BCSI. As required in CIP-011-2 Requirement R1, Part 1.2, Responsible Entities must implement procedures for protecting and securely handling BCSI in storage, transit, and use. One such procedure could include a procedure for preventing unauthorized access to BCSI. The principles below provide guidance to CMEP staff when evaluating program elements regarding access, such as access control and access authorization, in the protection of BCSI.

[1] The ERO Enterprise consists of NERC and the Regional Entities

[2] The ERO Enterprise Compliance Guidance Policy is located on the NERC website at: http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf

[3] Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a Standard that are vetted by industry and endorsed by the ERO Enterprise. CMEP Practice Guides differ from Implementation Guidance in that they address how ERO Enterprise CMEP staff executes compliance monitoring and enforcement activities, rather than examples of how to implement the Standard.

- Depending on the registered entity's facts and circumstances, CMEP staff should consider access to include any instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.
- When reviewing a registered entity's access controls, CMEP staff should consider whether there is a restriction on the ability for any individual to obtain and use BCSI. This restriction would be considered an access control. Such documented access controls must remain effective regardless of the BCSI state, whether in transit, in use, or at rest. As a best practice, a combination of preventative, detective, and corrective controls provides the greatest assurance of protection in both the physical and electronic realms.
- Access authorization relies on the registered entity to determine which individuals or groups need the ability to obtain and use the information and to create a process to grant approval. CIP-004-6 Requirement R4, Part 4.1.3 requires an access authorization process and requires the registered entity to base this determination for access authorization upon need.

Scenarios

This practice guide provides examples of access authorization (CIP-004-6 Requirement 4, Part 4.1) to physical and electronic BCSI and examples of access controls that may be part of the registered entity's CIP-011-2 Requirement R1 implementation. CMEP staff should consider the scenarios below to gain a better understanding of the registered entity's BCSI access authorization and protection processes, if applicable to the registered entity's particular circumstances. CMEP staff must audit the authorization process implemented by the registered entity for validity and effectiveness in each case separate from the protection processes. This categorical auditing methodology prevents confusion between the procedures to protect and securely handle BCSI (CIP-011-2) and the process to authorize access (CIP-004-6). The following scenarios and topics do not constitute a comprehensive analysis checklist but should serve as a guideline to drive to deeper understanding of the registered entity.

Scenario 1 – Physical BCSI

Physical BCSI may include, without being limited to, physical printouts of Electronic Security Perimeter diagrams, EOP-004 through EOP-011 required Emergency Preparedness and Operations processes with BES Cyber Asset passwords, etc.

- For CIP-011-2 Requirement R1, Part 1.2: CMEP staff should consider how the registered entity implemented its procedure(s) for protecting and securely handling BCSI, including storage, transit, and use.
- For CIP-004-6 Requirement R4, Part 4.1.3: CMEP staff should consider the registered entity's process and evidence to authorize access to physical BCSI storage locations.
- For CIP-004-6 Requirement R2, Part 2.1.5: CMEP staff should consider the registered entity's training program for the handling of BCSI and its storage locations. This may include policies,

access controls, and procedures that focus on the handling of BCSI during storage while in transit, and use.

- For CIP-004-6 Requirement R5, Part 5.3: CMEP staff should consider the registered entity's process in place to revoke access to designated physical BCSI storage locations by the end of the next calendar day following the effective date of a termination action.
- For CIP-004-6 Requirement R4, Part 4.4: CMEP staff should consider how the responsible entity performs and documents the required 15 calendar month review for the following:
  - Configured physical access control privileges;
  - Dated physical access authorizations; and,
  - Dated evidence demonstrating that existing physical access authorizations are correct and the minimum necessary to perform assigned work functions.

Scenario 2 – Electronic BCSI

Electronic BCSI may include, but is not limited to, electronic copies of security procedures or security information about BES Cyber Systems, collections of network addresses, and network topology of the BES Cyber System.

- For CIP-011-2 Requirement R1, Part 1.2: CMEP staff should consider the registered entity's procedures and evidence around controls that protect electronic BCSI in storage, use, and transit. For example, registered entities may demonstrate the implementation of effective technical controls such as the BCSI encryption and key management program. These controls could be considered access controls. While key management programs may vary, they must adhere to confidentiality and revocation principles. CMEP staff should review whether key management practices were implemented based on current industry recognized cryptographic best practices.
- For CIP-004-6 Requirement R4, Part 4.1.3: CMEP staff should consider the registered entity's processes and evidence used to authorize electronic access to electronic BCSI storage locations. This may include reviewing the registered entity's encryption key management, if used for BCSI protection.
- For CIP-004-6 Requirement R2, Part 2.1.5: CMEP staff should consider the registered entity's development of a training program for the handling of BCSI and its storage locations. This may include policies, access controls, and procedures that focus on the handling of BCSI during storage while in transit, and use.
- For CIP-004-6 Requirement R5, Part 5.3: CMEP staff should consider the registered entity's process in place to revoke access to designated electronic BCSI storage locations by the end of the next calendar day following the effective date of a termination action.
- For CIP-004-6 Requirement R4, Part 4.4: CMEP staff should consider how the responsible entity performs the required 15 calendar month review for the following:
  - Configured electronic access control privileges;

- Dated electronic access authorizations, including authorization for keys to encryption if used; and,
- Dated evidence demonstrating that existing electronic access authorizations are correct and the minimum necessary to perform assigned work functions.

Conclusion

In assessing a registered entity's access controls, CMEP staff should consider whether the ability to both obtain and use the BCSI has been met in order to have "access" to the BCSI. Additionally, CMEP staff should consider whether a registered entity's process upholds the principles of confidentiality and integrity, which *may* be accomplished by controlling access. During this review, CMEP staff should consider whether one type of access control, such as encryption along with key management, meets the security objective of CIP-011-2 Requirement R1, which is the prevention of unauthorized access to BCSI.

The NERC Reliability Standards covered in this Practice Guide establish the minimum controls for protecting BCSI information and CMEP staff must gain a better understanding of how each of the registered entity's various CIP programs are applied such as policies, procedures, access controls, training and periodic reviews with the ultimate goal of preventing unauthorized access to BCSI.