NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise CMEP Practice Guide

Network Monitoring Sensors, Centralized Collectors, and Information Sharing

Background

To support successful implementation 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 – (1) Implementation Guidance and (2) Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.[3] This document summarizes some of the requirements in NERC Reliability Standards, but the language of the Reliability Standards is enforceable and supersedes any description in this document.

Purpose

On April 20, 2021, the Department of Energy (DOE) launched an initiative, referred to as the 100- day plan, to enhance the cybersecurity of electric utilities' industrial control systems (ICS) and secure the energy sector supply chain. As part of the 100 day plan, DOE is seeking to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for ICS of electric utilities. As stated in DOE's press release, the initiative modernizes cybersecurity defenses and:

- Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities;
- Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real time situational awareness and response capabilities in critical ICS and operational technology (OT) networks;
- Reinforces and enhances the cybersecurity posture of critical infrastructure information technology networks; and
- Includes a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems.

As the ERO anticipates increased deployment of the technologies encouraged in the 100-day plan in environments subject to the CIP standards, the ERO identified a need to provide additional clarity and

[1] The ERO Enterprise consists of NERC and the six Regional Entities.
[2] The ERO Enterprise Compliance Guidance Policy is located on the NERC website at: https://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.

ensure a common approach to auditing compliance with the Critical Infrastructure Protection (CIP) Reliability Standards when a registered entity deploys detection and monitoring technologies that include, for instance, network monitoring sensors and centralized data collectors, and may involve the sharing of collected data. The purpose of this CMEP Practice Guide is to provide guidance to ERO Enterprise CMEP staff (CMEP staff) during the review and compliance assessment of a registered entity's network monitoring systems and information sharing practices.

During a compliance monitoring engagement, entity-specific facts and circumstances are to be considered by CMEP staff when assessing risks and compliance determinations. Risk information can be used to inform CMEP staff's understanding of a registered entity (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.

Overview

In assessing the application of the CIP Standards to many network monitoring solutions, there are two central issues that CMEP staff shall consider:

1. *Protection of the Device (Sensor):*
    a. Applicability question: Whether the deployment of the sensor in a registered entity's environment triggers the application of certain CIP requirements.
    b. If yes, whether the Registered Entity identified which requirements apply and determined how it plans to protect that device consistent with those requirements.
2. *Protection of the Data:*
    a. Applicability question: Whether the type of data being collected by and transmitted to a third-party (e.g., managed service provider (MSP)) triggers the need to protect that data and the Cyber Assets that process/store that data under the CIP standards.
    b. If yes, whether the Registered Entity identified which requirements apply and how it plans to protect and securely handle the data and the Cyber Assets that process/store that data consistent with those requirements.

Protection of the Cyber Asset(s)

The CIP standards require registered entities to protect Bulk Electric System (BES) Cyber Systems and certain associated Cyber Assets. The initial step in understanding the manner in which the CIP standards apply to network monitoring deployments is to determine whether the sensor to be deployed is a Cyber Asset, BES Cyber Asset, and then a BES Cyber System or other type of Cyber Asset subject to requirements of the CIP standards, such as a Protected Cyber Asset (PCA) or Electronic Access Control or Monitoring System (EACMS). As explained below, whether and the extent to which the sensor is itself subject to CIP requirements depends on which environments it will be deployed, the manner in which it is deployed in those environments, and the function(s) it performs in those environments. For instances where the registered entity may not own the sensors and/or monitoring device(s), the registered entity is still

responsible to demonstrate compliance based on function, location, and manner it is deployed. CMEP staff will consider these factors in assessing a registered entity's application of the CIP standards.

Categorization of Sensor(s)

- *Could the sensor be a BES Cyber Asset*? CMEP staff shall assess the sensor to determine if it meets the BES Cyber Asset categorization. Typically, based on the function it is performing, the sensor is unlikely to meet the definition of a BES Cyber System. However, CMEP staff should assess the registered entity's CIP-002 categorization process to ensure that the sensor would not meet the definition of BES Cyber System[4].
- *Is the sensor another type of device subject to CIP requirements? This depends on the environment in which it is deployed, the manner in which it is deployed in those environments, and its function(s).*
  - The initial questions CMEP staff must consider is whether the sensor will be deployed in an environment that contains high, medium, or low impact BES Cyber Systems (as determined in accordance with Attachment 1 to CIP-002 for the impact level criteria).
  - If the sensor is being deployed in High or Medium Impact Environments:
    - If the sensor is connected using a routable protocol within or on an Electronic Security Perimeter (ESP), CMEP staff should assess whether it should be categorized as a Protected Cyber Asset (PCA), as that term is defined in the NERC Glossary, and the requirements associated with the particular impact level would apply.
    - If the sensor performs certain electronic access and/or access monitoring activity, CMEP staff should assess it as possibly an Electronic Access Control or Monitoring System (EACMS) and be subject to the requirements associated with the particular impact level.
      - CMEP staff would need to better understand the functions performed by the sensor to assess whether it would be an EACMS.
      - If, for instance, the sensor is used to passively collect traffic from a configured SPAN or Mirror port on a managed switch, within or on the ESP, and then transmit the collected data to a centralized data collector for further analysis in order to comply with CIP-005-6, CIP-007-6, or CIP-010-3, it may qualify as an EACMS. However, location within the ESP would also require PCA classification and require all PCA protections as set forth in the CIP Requirements.
    - If the sensor is being deployed in an environment with high or medium impact BES Cyber Systems but would not be located within, or on, an ESP, CMEP staff should assess the sensor for EACMS applicability.
      - Note that if the sensor is located outside an ESP but communicates with BES Cyber Systems or other devices within an ESP, CMEP staff should assess the registered entity's CIP applicability evaluation and whether the registered entity applied any required

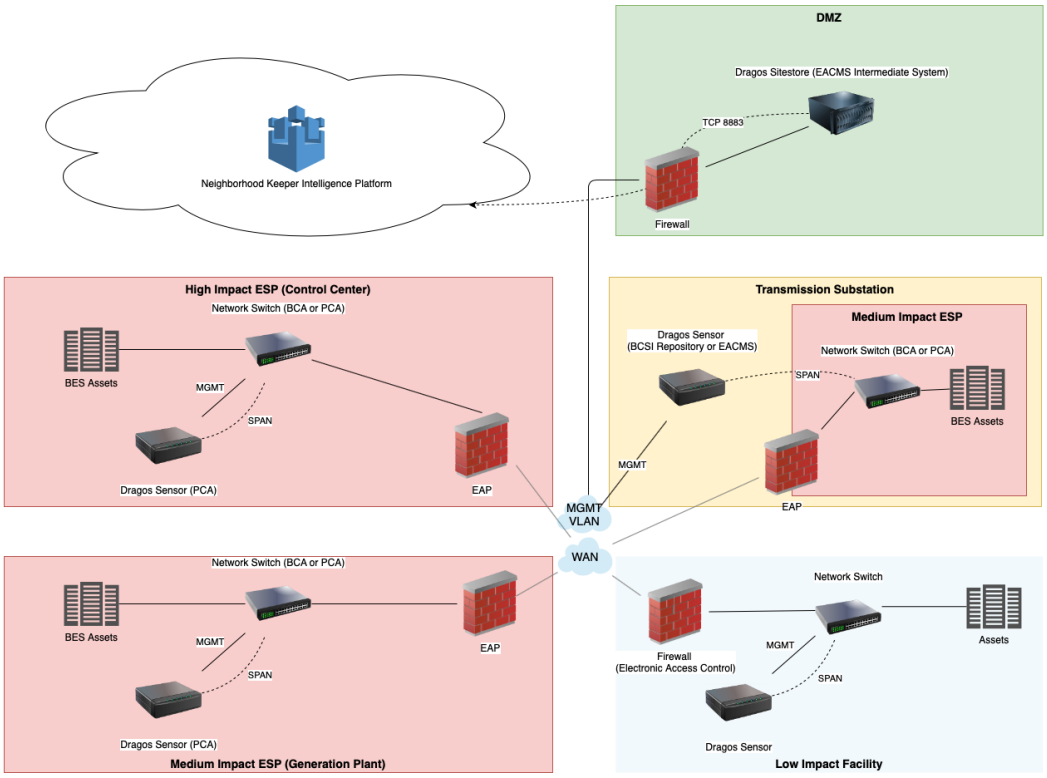
[4] https://www.nerc.com/files/glossary_of_terms.pdf

protections applicable to that communication. If, however, the sensor management interface is outside the ESP and the SPAN port is connected to a switch within the ESP, the Sensor is not communicating with BES Cyber Systems or other devices within an ESP, possibly exempting it from applying protections other than those required for designated storage locations for BCSI.

- Low Impact Environments
  - If the sensor is deployed in an environment with only low impact BES Cyber Systems, the sensor may be performing the functions of an EACMS, or other category of device subject to the CIP standards; however, CMEP staff should assess whether these devices are subject to CIP-003. Those categories of devices are not categories of assets applicable to requirements for low impact assets. Under this scenario, registered entities would not have to apply protections to the device itself, although they may still be responsible for complying with the electronic access control requirements applicable to assets containing low impact BES Cyber Systems and data protection requirements, discussed below.

If the sensor would be deployed in, or on, an ESP that contains high and medium impact BES Cyber Systems, the sensor would be a PCA or an EACMS, the remaining paragraphs are an initial identification of requirements that CMEP staff will assess. Reference Figure 1 provides several examples of how the sensors and/or data collectors may be deployed. There may be other deployment options, but these are the typical installations.

Dragos Neighborhood Keeper Sample Diagram: Combination with Management Outside ESP



Application of Electronic Access Control Requirements

- If the sensor is a low impact BES Cyber Asset, CMEP staff should assess whether CIP-003 electronic access control requirements have been applied if there is routable protocol entering or leaving the asset containing the low impact BES Cyber System(s).
- For high and medium BES Cyber Systems and their associated PCAs and EACMS, CMEP staff should assess the CIP-004 access controls, which require an access management program that includes authorizations, training, and background checks. In addition, CMEP staff should assess the CIP-004 authorization requirements for BCSI designated storage locations.
- In instances where the registered entity is deploying the sensor to an asset that contains high or medium impact rating BES Cyber Systems, CMEP staff should assess whether the registered entity identified those individuals/organizations that will have access to the sensor and the manner in which the registered entity will incorporate them into their access control processes.
- If the registered entity uses a MSP or other type of vendor for its deployment, CMEP staff should confirm whether any of those third-party personnel have electronic access to the on premise equipment associated with the deployment. If third-party personnel do not have electronic access to the on premise equipment, CMEP staff should verify the existing CIP-003 and CIP-004 policies

and procedures to the equipment for which the registered entity personnel have access. If third-party personnel do have electronic access, CMEP staff should verify if those personnel were included in the registered entity's existing access management and revocation policies and procedures.

Application of Electronic Security Perimeter Requirements

- For instances where the registered entity deploys the sensor within an environment that is subject to CIP-005, CMEP staff should determine if the registered entity implemented controls to demonstrate compliance related to ESPs and Interactive Remote Access (IRA). The evaluation must be done for the sensor and its placement within, or on, the ESP.
- To understand the application of these requirements, CMEP staff should assess whether the registered entity identified and documented the inbound and outbound access permissions and reason for granting access.
- If the sensor is classified as a high or medium impact BES Cyber System, or associated PCA, CMEP staff should assess if the registered entity identified who will have IRA to the sensor, within the ESP, and security controls around that access. CIP-005 requires all IRA to be routed through an Intermediate System. CMEP staff should assess the vendor remote access session data flow (including IRA and system- to-system remote access), including associated ports and services.
- If the registered entity uses an MSP or other type of vendor for its deployment, CMEP staff should confirm whether any of those third-party personnel, or vendors, have remote access (IRA or system-to-system) to the on-premises equipment associated with the deployment.

Application of System Security Management Requirements

- CMEP staff should determine how the registered entity complies with CIP-007, which includes system security management requirements applicable to high and medium impact BES Cyber Systems, and their associated PCAs and EACMS (e.g., disabling ports; applying security patches; malicious code prevention; security event monitoring; and system access controls).
- CMEP staff should assess whether the registered entity included the network monitoring solution in its current security patch management program. In addition, CMEP staff would need to understand the patch source for the sensor, plans for implementing patches, and the registered entity's process for implementing mitigating activities for instances where patches cannot be installed.

Change Management and Vulnerability Assessments

- CMEP staff should assess the registered entity's CIP-010 controls. CIP-010 requires registered entities to conduct vulnerability assessments and have a change management process for high and medium impact BES Cyber Systems and associated PCAs and EACMS. This includes establishing a baseline, verifying the baseline, documenting changes to the baseline and monitoring for changes to the baseline. CMEP staff should determine how the network monitoring systems are compliant with those requirements, if applicable.

- CMEP staff is responsible for assessing compliance and the registered entity is expected to demonstrate how it complies with these requirements for the deployment within their specific environments. Specifically, CMEP staff should understand how the registered entity would maintain the baseline and verify that cyber security controls were not adversely affected following changes. In most cases, registered entities could apply their existing controls to the deployed technology, ensuring that they maintain the baseline and that CIP-005 and CIP-007 controls are not adversely impacted.

Supply Chain Risk Management

- CMEP staff should assess CIP-013 and the required registered entities' controls to mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems. This includes initial procurement and continuing support contracts that address the processes used in procuring, installing, and supporting the Cyber Assets deployed within a registered entity's specific environments.
- CMEP staff should assess how the registered entity complies with these requirements and how the registered entity implemented its supply chain cyber security risk management plan specified in CIP-013. In most cases, registered entities could apply their existing controls showing correspondence, policy documents, or working documents that demonstrate inclusion of the vendor into the CIP-013 program.

Protection of Data

Under the CIP standards, registered entities must apply controls to protect BES Cyber System Information (BCSI), which is defined as:

> *Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.*

CMEP staff should assess how the registered entity determined whether the data collected by the sensors and/or the centralized data collector includes BCSI, and whether the data would be transmitted to third parties.

If the sensor captures BCSI, CMEP staff would need to assess the following standards applicable to BCSI:

- CIP-004 Requirement R4 Part 4.1 – requires registered entities to have a process in place to authorize, based on need, access to designated storage locations, whether physical or electronic, for BES Cyber System Information.[5]
- CIP-011 Requirement R1 Part 1.2 – requires registered entities to have a process for identifying BCSI, protecting, and securely handling BCSI, including storage, transit, and use. The process should include how the registered entity addresses providing BCSI to third party vendors or other recipients. Depending on the implementation, CMEP staff should verify that the third-party vendor has also applied the necessary protections to the devices that contain BCSI.

In some implementations, the registered entity may anonymize data to send to third-party vendors. For instance, some of network monitoring solutions strip the data of all identifying information and potentially sensitive information such as host IP addresses, MAC addresses, and hostnames. In those instances, CMEP staff should obtain reasonable assurance that the BCSI requirements may not apply to the transmission of data to the third party. CMEP staff should ask the registered entity to provide documented processes, demonstrating how the data is anonymized and specify what data is actually transmitted to the third party.

Conclusion

In assessing a registered entity's network monitoring deployment, CMEP staff should consider the specific facts and circumstances for each aspect of the deployment. For example, CMEP staff should assess the registered entity's deployment of the network monitoring sensors, the centralized data collector, and data protection to include how, or when, data is shared with third parties. During a review, CMEP staff should assess the protection of the devices as well as the protection of the data.

The NERC Reliability Standards covered in this Practice Guide establish a set of controls for protecting network monitoring deployments and BCSI information. During compliance monitoring engagements, CMEP staff must understand 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 these Cyber Assets as well as any associated BCSI.

[5] The ERO Enterprise released a Practice Guide to assess a registered entity's access controls specifically to the data, not necessarily the storage locations. NERC compliance monitoring staff will assess the facts and circumstances of who has the ability to both obtain and use the BCSI to uphold the principles of confidentiality and integrity, which may be accomplished by controlling access to the data. https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf

Revision History

Revision #	Revision Date	Revision Details
V0.1	June 4, 2021	Initial Draft