2024

Lessons Learned from Commission-Led CIP Reliability Audits

FEDERAL ENERGY REGULATORY COMMISSION
Office of Electric Reliability
Division of Cyber Security

2024
Lessons Learned from Commission-Led CIP Reliability Audits

A Staff Report

August 26, 2024

FEDERAL ENERGY REGULATORY COMMISSION
Office of Electric Reliability
Division of Cyber Security

TABLE OF CONTENTS

INTRODUCTION

During Fiscal Year (FY) 2024,[1] staff of the Federal Energy Regulatory Commission (Commission) completed non-public Critical Infrastructure Protection (CIP) Audits (CIP Audits) of several U.S.-based North American Electric Reliability Corporation (NERC) registered entities.[2] The CIP Audits evaluated registered entities' compliance with the applicable Commission-approved CIP Reliability Standards (CIP Standards).[3] Staff from NERC and the Regional Entities participated in the CIP Audits, including the virtual and on-site portions.

During the CIP Audits, staff found that while most of the cyber security protection processes and procedures adopted by the registered entities met the mandatory requirements of the CIP Standards, potential noncompliance and security risks remained. Staff also identified practices not required by the CIP Standards that could improve security, which this report includes as voluntary cyber security recommendations.[4]

This anonymized summary report informs the regulated community and the public of lessons learned from the FY2024 CIP Audits. This report provides information and recommendations to NERC, Regional Entities, and registered entities for use in their assessments of risk and compliance, and to improve overall cyber security. Moreover, this information may be generally beneficial to the utility-based cyber security community to improve the reliability and security of the Bulk-Power System.[5]

1 The fiscal year is the accounting period for the federal government that begins on October 1st and ends on September 30th. The fiscal year is designated by the calendar year in which it ends; for example, FY2024 began on October 1, 2023, and ended on September 30, 2024.

2 Section 215 of the Federal Power Act (FPA) gives NERC (as the Commission-certified Electric Reliability Organization (ERO)) the authority to establish and enforce Reliability Standards for users, owners, and operators of the Bulk-Power System. The Reliability Standards are subject to Commission review and approval. 16 U.S.C. § 824o. Entities are registered in accordance with the NERC Rules of Procedure. *See* NERC, *Rules of Procedure*, https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

3 Compliance with Commission-approved Reliability Standards is mandatory and enforceable for all applicable registered entities pursuant to section 215 of the FPA, 16 U.S.C. § 824o. *See also* 18 C.F.R. § 39.2(a).

4 The Commission's Office of Energy Infrastructure Security (OEIS) was not involved in these audits. However, the Office of Electric Reliability consulted with OEIS regarding these practices for the purposes of this report. OEIS is not responsible for the development or enforcement of CIP Standards but instead is responsible for the identification and sharing of best practices to address current and emerging defense and mitigation strategies for advanced cyber and physical threats to, not only the Bulk-Power System, but all energy infrastructure under the Commission's jurisdiction.

5 The Bulk-Power System is defined in the FPA as facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. 16 U.S.C. § 824o(a)(1).

CIP RELIABILITY STANDARDS

Section 215 of the FPA provides that the Commission may certify an ERO, the purpose of which is to establish and enforce Reliability Standards, which are subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[6] The Commission established a process to select and certify an ERO,[7] and subsequently certified NERC as that ERO.[8]

The CIP Standards are designed to mitigate the cyber security and physical security risks to bulk electric system (BES)[9] facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable because of a security incident, would affect the reliable operation of the Bulk-Power System. Pursuant to section 215 of the FPA, on January 28, 2008, the Commission approved an initial set of eight mandatory CIP Standards pertaining to cyber security.[10] In addition, the Commission directed NERC to develop certain modifications to the CIP Standards. Since 2008, the CIP Standards have undergone multiple revisions to address Commission directives and respond to emerging cyber security issues.[11]

The Commission initiated its CIP Standards audit program for registered entities in FY2016, and the Commission has conducted CIP Audits each year since.

The CIP Standards may be found on NERC's website. Specific CIP Standards referenced in this report can be found with the following links:

1. CIP-002-5.1a – Cyber Security - BES Cyber System Categorization
2. CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
3. CIP-011-2 – Cyber Security – Information Protection
4. CIP-012-1 – Cyber Security – Communications between Control Centers

---

6 16 U.S.C. § 824o.

7 *Rules Concerning Certification of the Elec. Reliability Org.; & Procs. for the Establishment, Approval, and Enf't of Elec. Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

8 *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,190, *order on reh'g*, 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

9 NERC's Commission-approved BES definition is a subset of the Bulk-Power System and one method NERC uses to identify the facilities and elements necessary for the reliable operation and planning of the interconnected Bulk-Power System and the entities subject to NERC compliance. Generally included within the BES definition are those elements of the Bulk-Power System that are operated or connected at 100 kV or higher. Other elements or facilities may be added or removed from the BES definition based on application of various inclusions and exclusions that are a part of the definition. *See*, *Revisions to Elec. Reliability Org. Definition of Bulk Elec. Sys. and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012), *order on reh'g*, Order No. 773-A, 143 FERC ¶ 61,053 (2013).

10 *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *denying reh'g and granting clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

11 *See e.g.*, *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014); *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, *order denying reh'g*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

AUDIT SCOPE AND METHODOLOGY

Audit fieldwork consisted of data requests and reviews, webinars and teleconferences, virtual and on-site visits. Prior to the virtual and on-site visits, staff issued data requests to gather information pertaining to entities' CIP activities and operations and held webinars and teleconferences to discuss the audit scope and objectives, data requests and responses, technical and administrative matters, and compliance concerns.

During the virtual and on-site visits, staff:

1. interviewed the entities' subject matter experts and observed demonstrations of its staff's operating practices, processes, and procedures;

2. interviewed employees and managers responsible for performing tasks within the audit scope and analyzed documentation to verify compliance with CIP Standard requirements;

3. conducted several field inspections remotely and observed the functioning of applicable Cyber Assets[12] identified by the registered entity as High, Medium, or Low Impact;[13] and

4. interviewed compliance program managers, staff, and employees responsible for day-to-day compliance.

Applicable Cyber Assets consisted of BES Cyber Assets[14] that compose a BES Cyber System,[15] and associated Cyber Assets to that BES Cyber System. Associated Cyber Assets consist of Electronic Access Control or Monitoring Systems (EACMS),[16] Physical Access Control Systems (PACS),[17] and Protected Cyber Assets (PCAs).[18]

The data, information, and evidence provided by the entities were evaluated for sufficiency, appropriateness, and validity. Documentation submitted in the form of policies, procedures, e-mails, logs, studies, and data were validated and substantiated as appropriate. For certain CIP Standards' requirements, sampling was used to assess compliance.

---

12 Cyber Assets refer to programmable electronic devices, including the hardware, software, and data in those devices. NERC, *Glossary of Terms Used in NERC Reliability Standards*, at 10, (May 8, 2024), https://www.energy.gov/sites/prod/files/2017/09/f36/NERC%20Glossary.pdf (NERC Glossary).

13 The CIP Standards require that applicable registered entities categorize their BES Cyber Systems and associated Cyber Assets as High, Medium, or Low Impact according to the criteria found in Reliability Standard CIP-002-5.1a - Attachment 1.

14 A BES Cyber Asset is a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES. Redundancy of affected facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. *See* NERC Glossary at 5.

15 A BES Cyber System is one or more BES Cyber Assets logically grouped by an entity to perform one or more reliability tasks for a functional entity. *Id.* at 5.

16 EACMS are "Cyber Assets that perform electronic access control or electronic access monitoring of the [ESP] or BES Cyber Systems. This includes Intermediate Systems." *Id.* at 12. There are five basic types of EACMS: (1) Electronic Access Points (e.g., firewalls); (2) Intermediate Systems (e.g., remote access systems); (3) Authentication Servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities); (4) Security Event Monitoring Systems; and (5) Intrusion Detection/Prevention Systems. Reliability Standard CIP-002-5.1a (Cyber Security - BES Cyber System Categorization) at 6.

17 PACS are Cyber Assets that control, alert, or log access to the Physical Security Perimeter, exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. *Id.* at 22.

18 Protected Cyber Assets are Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter (ESP) that are not part of the highest impact BES Cyber System within the same ESP. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. Put simply, a Protected Cyber Asset is a Cyber Asset that works within a logical network of a BES Cyber Asset but is not itself a BES Cyber Asset. *Id.* at 23.

OVERVIEW OF LESSONS LEARNED

The lessons discussed in this report are intended to help registered entities improve their compliance with the CIP Standards and are presented in numerical order by CIP Standard:

1. CIP-002-5.1a, R1: Assess the risk to operations presented by associated Cyber Assets, such as EACMS, PCAs, and PACS, and consider additional security controls beyond those that are required by their categorization.

2. CIP-002-5.1a, R1: Ensure logically segmented Control Centers at a single site location are evaluated as a single Control Center in BES Asset identification and categorization procedures.

3. CIP-010-4, R1.1.2: Ensure that Cyber Asset baselines include all intentionally installed, commercially available software on each Cyber Asset, including browser extensions and standalone applications.

4. CIP-011-2, R1: Identify, monitor, and implement controls to protect BES Cyber System Information (BCSI) to mitigate the risks posed by unauthorized disclosure and unauthorized access.

5. CIP-012-1, R1: Ensure the risks of unauthorized disclosure and unauthorized modification of real-time data transmitted between Control Centers within a single environment (Networks, ESPs, etc.) are identified and addressed.

LESSONS LEARNED DISCUSSION

BES Cyber System Asset Identification and Categorization

CIP-002-5.1A, REQUIREMENT R1

Overview

Assess the risk to operations presented by associated Cyber Assets, such as EACMS, PCAs, and PACS, and consider additional security controls beyond those that are required by their categorization. Reliability Standard CIP-002-5.1a Requirement R1 requires entities to identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the Bulk-Power System. To identify and categorize these systems and assets, entities refer to the Reliability Standard's Attachment 1, which defines the criteria for each impact rating. Pursuant to Reliability Standard CIP-002-5.1a, Attachment 1, BES Cyber Systems and associated BES Cyber Assets may be classified as Low, Medium, or High impact.

Background

While entities generally had strong processes and procedures for the identification of their BES Cyber Systems and associated Cyber Assets, in some cases there were associated Cyber Assets that posed additional operational risks, beyond those implied by their categorization, based on the distinct system architecture they supported. Specifically, instances existed where entities deployed "next-generation firewalls"[19] that were configured in such a manner that their loss, compromise, or misuse may cause a "15-minute impact"[20] to the reliable operation of the BES beyond what is suggested by their categorization as EACMS.

Risk

Audit staff learned from discussions with entity staff, that should these EACMS devices (or similarly functioning associated cyber assets) fail to work as intended, they may fail "closed" - meaning that network traffic will no longer be able to flow as required for normal network behavior. This scenario presents a high likelihood that an entity would encounter difficulty using their systems to perform expected BES reliability operating services.[21] While it is unlikely that an entity can mitigate every possible risk event, applying additional controls to address specific failure scenarios is prudent to minimize the risk to the real-time reliable operation for the Bulk-Power System. These devices sit outside of the ESP and therefore do not meet the definition of BES Cyber Asset by design; however, they may support BES Cyber Assets in a manner that suggests higher criticality than the security controls required to be implemented by the CIP Standards.

---

19 Next-generation firewalls expand upon prior firewall technologies by adding features such as application filtering, deep packet inspection, VPN traffic awareness, adaptive rules, and threat detection. *See*, Nat. Inst. of Standards and Tech., *NIST SP 800-82r3: Guide to Operational Technology (OT) Security*, Appendix E, Section E.1.1., at 207, (September 2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf.

20 *See* NERC Glossary definition of BES Cyber Asset at fn 14, *supra*.

21 BES Reliability Operating Services includes several named services, including Dynamic Response to BES Conditions, Balancing Load and Generation, Controlling Frequency (Real Power), Controlling Voltage (Reactive Power), Managing Constraints, Monitoring & Control, Restoration of BES, Situational Awareness, and Inter-Entity Real-Time Coordination and Communication. Reliability Standard CIP-002-5.1a (Cyber Security - BES Cyber System Categorization) at 17.

The identification and categorization of BES Cyber Systems is foundational to the CIP Standards. While miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate (or non-existent) cyber security controls, so too can correct asset categorization without a specific lens applied to the criticality of that asset within the specific system architecture it supports. Misunderstanding the functions and criticality of an asset can ultimately affect the real-time operation of the BES by virtue of lacking fully appropriate security controls that meet the specific operational needs of an entity.

Mitigation

Entities should consider enhancing their identification and categorization procedures to better identify and categorize their BES Cyber Systems in the following ways:

Consider broadening the concept of "15-minute impact" from the NERC Glossary definition of "BES Cyber Asset" to associated Cyber Assets (e.g., EACMS) that may pose enhanced risk beyond their initial categorization. This consideration can be used to inform the application of additional security controls that support all the necessary functioning of the systems those assets support. Examples of controls that may be useful to apply to an EACMS in this situation, that would normally be reserved for BES Cyber Assets, include:

a. CIP-005-7 (Electronic Security Perimeter), Requirements R2.4 and R2.5

b. CIP-009-6 (Recovery Plans for BES Cyber Systems), Requirement R2.3 for both High and Medium Impact BES Cyber Systems

During the system design process, consider the principles of least privilege and implementing systems that contain the least complexity necessary to achieve the reliability objectives inherent to the entity's registered functions.

Control Center Categorization

CIP-002-5.1A, REQUIREMENT R1

Overview

Ensure logically segmented Control Centers[22] at a single site location are evaluated as a single Control Center in BES Asset identification and categorization procedures. Reliability Standard CIP-002-5.1a Requirement R1 requires entities to identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the Bulk-Power System. BES Cyber Systems and associated BES Cyber Assets may be classified as Low, Medium, or High impact.

Background

Audit staff found that in BES Asset identification and categorization procedures, some entities inappropriately segmented their single Control Center into multiple Control Centers that shared the same physical building and infrastructure but were logically segmented by electronic access controls.

Risk

Reliability Standard CIP-002-5.1a, Attachment 1, Criterion 2.1 requires entities to identify each BES Cyber System comprising an associated commissioned generation asset with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1,500 MW in a single interconnection as medium impact. To reduce the compliance risk associated with the medium impact CIP Reliability controls, audit staff observed that some entities logically segmented their single Control Center into multiple control centers, each falling under the 1,500 MW threshold.

These entities were not fully aware of the limitations of segmentation within the CIP Standards. The CIP Standards allow the flexibility to logically segment BES Cyber Systems, for example logically separating a generation asset's units to lower the single site generation below 1,500 MW. However, in this instance the NERC Glossary definition of Control Center does not allow that type of segmentation to occur because the definition already encompasses "one or more facilities. . .".[23]

Identification and categorization are foundational to the CIP Reliability Standards. Failure to properly categorize BES Cyber Systems with the appropriate impact rating means that an entity may not apply the required controls consistent with the risk, consequently impacting the reliable operation of the Bulk-Power System. For example, if common infrastructure (e.g., a backup system) is shared across a segmented Control Center, the overarching criteria (or control) should be applied to the common infrastructure.

22 A "Control Center" is one or more facilities hosting operating personnel that monitor and control the BES in real-time to perform the reliability tasks, including the associated data centers, of: (1) a Reliability Coordinator, (2) a Balancing Authority, (3) a Transmission Operator for transmission Facilities at two or more locations, or (4) a Generator Operator for generation Facilities at two or more locations. *See* NERC Glossary at 10.

23 *See* NERC Glossary at 10.

Mitigation

Entities should consider the physical component in addition to the logical separation of the assets within its network when identifying their Control Centers. For example, if a Control Center is housed within the same physical boundary, it should be considered one Control Center.

Additional Guidance

NIST SP 800-53r5 discusses separation in terms of critical components, recommending a defense-in-depth protection strategy by "determin[ing] the degree of physical separation of system components. Physical separation options include physically distinct components in separate racks in the same room, critical components in separate rooms, and geographical separation of critical components."[24]

24 NIST, SP 800-53r5: *Security and Privacy Controls for Information Systems and Organizations*, at 320-321, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Baseline Reporting of Browser Extensions and Standalone Applications

CIP-010-4 REQUIREMENT R1. PART 1.1.2

Overview

Ensure that Cyber Asset baselines include all intentionally installed, commercially available software on each Cyber Asset, including browser extensions and standalone applications. Reliability Standard CIP-010-4, Requirement R1., Part 1.1 requires entities to baseline commercially available or open-source application software that are intentionally installed (i.e., knowingly, and purposefully installed by the entity and/or by a delegate at the entity's direction). The baselining of Cyber Assets and configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Background

Audit staff found that while entities generally included baselines of commercially installed software on each Cyber Asset, in some cases entities did not include or could not differentiate between the browser extension or standalone version of the same software application. As stated in the technical rationale and justification for this requirement, software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration.[25]

Commercially available, open-source, installed software is required to be baselined by CIP-010-4 Requirement R1., Part 1.1.2. Entities generally use automated tools for baseline configurations but sometimes misreported installed-but-disabled software. Standalone software, even disabled for use, should be listed in the baseline, and marked as disabled.

Risk

Configuration Management is crucial for recovery and business continuity. When troubleshooting issues, reverting to previous versions associated with each change facilitates the process. Without baseline documentation or with incorrect documentation, restoring BES Cyber Systems to their prior configuration becomes challenging, if not impossible. Also, incomplete, or inaccurate documentation of baselines can result in an inaccurate assessment of the security posture.

Mitigation

Entities are required to develop a baseline configuration, individually or by group, which should include any commercially available or open-source application software (including its version) intentionally installed.

25 *See*, NERC, *Cyber Security – Configuration Change Management and Vulnerability Assessments*, at 15, (Oct. 2020), https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-010-4_Technical_Rationale_clean_10072020.pdf.

Entities should consider developing a Configuration and Change Management Plan that includes the following elements:[26, 27]

- Configuration item
- Baseline configuration or setting
- Configuration management database
- Configuration control review board

In addition, monitoring of the configuration changes should have a clear step of identifying disparities between authorized/approved baselines and actual/implemented baselines.

Additional Guidance

NIST SP 800-82r3 recommends the following practices:

- "Updating inventory information when components are added, removed, or changed (e.g., patched, new firmware installed, component swapped during maintenance) helps organizations accurately manage their overall environmental risks."[28]
- "Software and firmware inventory management to track the software and firmware installed with the Operational Technology (OT)[29] components, including version numbers, location information, and software bill of materials (SBOM)."[30]
- Maintaining an accurate inventory of the IT and OT assets within the environment of operation – including the product vendor, model numbers, firmware, OSs, and software versions installed on the assets – facilitates the identification, tracking, and remediation of vulnerabilities."[31]

---

26 *See*, *e.g.*, NIST, SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, at 20 (2011), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf.

27 *See*, *e.g.*, CISA, *CRR Supplemental Resource Guide: Configuration and Change Management*, Vol. 3, Ver. 1.1, at 5 (2016), https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-CCM.pdf.

28 *See*, *e.g.*, NIST, SP 800-82, *Guide to Operational (OT) Security*, Ver 3, at 91-94 (2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.TSP.800-82r3.pdf.

29 Operational Technology is defined as "A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems." *See,* Nat. Inst. of Standards and Tech., NIST SP 800-82r3: *Guide to Operational Technology (OT) Security*, Appendix B, at 165, (September 2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf.

30 Id.

31 Id.

BES Cyber System Information Protection

CIP-011-2, REQUIREMENT R1

Overview

Identify, monitor, and implement controls to protect BES Cyber System Information (BCSI) to mitigate the risks posed by unauthorized disclosure and unauthorized access. Reliability Standard CIP-011-2, Requirement R1.1, states that entities must [develop] "method(s) to identify information that meets the definition of BES Cyber System Information," and Reliability Standard CIP-011-2, Requirement R1.2, states that entities must develop "[p]rocedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use."

Background

Audit staff found that while entities generally implemented policies, procedures, and controls for BCSI and associated BES Cyber Systems, the process and implementation could be improved. In some cases, not all entities consistently implemented adequate controls to identify, protect, and securely handle BCSI.

Risk

Audit staff identified multiple instances of BCSI-related risk throughout the audits conducted during FY2024. Specifically, some entities could improve their BCSI information protection programs by: (1) implementing additional controls and practices to properly identify BCSI; and (2) improving controls to properly protect and securely handle BCSI. For example, some entities did not account for individuals who had access to BCSI. In some cases, these individuals did not have the need to know but were included in access groups. Most technologies used in support of access groups for shared drives have default administrator accounts built in that have full control to that shared drive by default. Entities should restrict access to the greatest degree possible to limit the likelihood of either accidental or purposeful improper information exposure. In addition, some entities did not apply proper controls for access to physical BCSI generated from printers within a physical security perimeter. In some instances, entities had policies and procedures for handling and protecting BCSI, but the implementation of stated controls did not align with the policy elements. For example, network diagrams containing BCSI were allowed to be printed but the controls used to implement the policy did not ensure that the information was stored safely or properly disposed of after use.

Identification and the implementation of security controls to properly protect and securely handle BCSI is a critical part of a successful information protection program. Failing to properly identify, track, document, and monitor information associated with a BES Cyber System as BCSI presents a risk of the unauthorized access or exposure of information.

Mitigation

Entities should consider the following areas to enhance BCSI information protection programs:

Physical Requirements:

1. Revise procedures and controls to comprehensively address monitoring and tracking of physical BCSI.

2. When identifying and documenting physical BCSI storage locations, consider where any printers are located and the ability to print hard copies.

3. Ensure cyber security training includes proper handling, identification, and use of BCSI.

Electronic Requirements:

1. Re-evaluate methods for identifying BCSI and associated BES Cyber Systems.

2. Review all data sources and ensure all BCSI is properly identified.

3. Re-evaluate BCSI access and protection measures.

Additional Guidance

As an example, consider digital projections of network diagrams that, while sensitive, are not labeled as such. The risk exists that the documents may be mishandled if they are printed or electronically distributed. Before viewing digital projections, the intended audience should be authorized to receive BCSI. The material presented should also be evaluated and marked with handling instructions appropriately. Guidance should be provided to all recipients of the data to ensure its proper handling.

NIST SP 800-53r5 recommends, "Impact-level prioritization and the resulting sub-categories of the system give organizations an opportunity to focus their investments related to security control selection and the tailoring of control baselines in responding to identified risks."[32]

32 *See, e.g.*, NIST, SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Ver 5, at 239 (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Control Center Real-Time Communications Identification

CIP-012-1, REQUIREMENT R1

Overview

Ensure the risks of unauthorized disclosure and unauthorized modification of real-time data transmitted between Control Centers within a single environment (Networks, ESPs, etc.) are identified and addressed. Entities did not identify, implement, or document plans to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-Time Access/Real-Time Monitoring (RTA/RTM)[33] data while being transmitted between its own internal applicable Control Centers. Reliability Standard CIP-012-1, Requirement R1, states that entities are responsible for developing a plan to mitigate the risks posed by unauthorized disclosure and unauthorized modification of data being transmitted between any applicable Control Centers. Requirement R1.1 states that the plan must include the "identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers," and Requirement R1.2 states that the plan must include the "identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers."

Background

Audit staff found that while entities generally had strong processes and procedures for the identification of RTA/RTM communications, some failed to recognize or categorize the communications paths internal to their own networks. Specifically, some entities did not consider the connection between their primary and backup control centers as applicable under the CIP-012-1 Reliability Standard because their Energy Management System (EMS) architecture did not appear at the surface-level to transmit RTA/RTM data through that communication link. For example, there are some EMS architectures that operate in a "hot/standby" configuration, whereby the primary control center has a hot, or active, server that is processing RTA/RTM data in production, while the EMS server at the backup control center waits in a standby configuration. This means that the backup server receives periodic data transmission from the primary server for synchronization purposes but is not actively processing data related to RTA/RTM. This type of EMS configuration led some entities to leave the communications path between their two Control Centers out of their protection plan under Reliability Standard CIP-012-1. Nevertheless, in some instances, like this example, entities did implement technical protections that were sufficient to meet the technical rationale of the Reliability Standard.

Audit staff, upon discussions with entities and review of implementation evidence during audit fieldwork, understood that in situations with similar EMS architectures as described here, the communications path should be considered in the scope of the CIP-012-1 Reliability Standard. The data transmitted for synchronization between a hot and standby server, even when not actively used in production under normal circumstances, is still RTA/RTM data and is of the same criticality regardless of which EMS node is processing the data at a point in time. Scenarios exist where either a control center may become physical unavailable, or the primary EMS node becomes unavailable, resulting in the potential for RTA/RTM to be sent across that communications link between control centers that will be used in production by operators.

33 RTA is "[a]n evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions." The definition explains that the evaluation uses inputs including, but not limited to "load; generation output levels; known Protection System and Remedial Action Scheme status or degradation, functions, and limitations; Transmission outages; generator outages; Interchange; Facility Ratings; and identified phase angle and equipment limitations." NERC Glossary at 24.

Risk

Failure to identify Control Center to Control Center communications, provide security protections for RTA/RTM data, as well defining an entity's roles in the transmission of RTA/RTM data can lead to data exposure for the communication paths between Control Centers. Not identifying the Control Center communications could lead to the compromise of sensitive data due to entities not applying the required security controls for the communications paths. Failure to clearly define responsibilities and roles for the transmission of RTA/RTM data could lead to improper handling (or integrity) of the communications.

Mitigation

Entities should enhance their identification of RTA/RTM communications not only to external Control Centers but include all Control Centers, including Control Centers within their own environments.

Additional Guidance

With regards to the identification of communication paths, staff also recommends that entities identify and isolate less critical communications from more sensitive operational technology (OT) networks. Systems and services that are assessed to not intersect with OT services and their associated network communications should be fully separated from the more sensitive OT network to reduce the attack surface.

NIST SP 800-82r3 recommends, "[t]he use of network segmentation and isolation should support an organization's OT cyber security defense-in-depth architecture… While [virtual local area networks] can be a cost-effective solution for OT network segmentation, organizations should consider utilizing physically separate switches for segmenting high-criticality devices, such as those that support safety systems."

2017-2023 PREVIOUS LESSONS LEARNED RECOMMENDATIONS

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
All	All	Enhance internal compliance and controls programs to include control documentation processes and associated procedures pertaining to compliance with the CIP Reliability Standards.	2021
All	All	Conduct a thorough review of CIP Reliability Standards compliance documentation; identify areas of improvement to include but not be limited to instances where the documented instructional processes are inconsistent with actual processes employed or where inconsistencies exist between documents; and modify documentation accordingly.	2017
All	All	Review communication protocols between business units related to CIP operations and compliance and enhance these protocols where appropriate to ensure complete and consistent communication of information.	2017
All	All	Consider the use of secure administrative hosts to perform administrative tasks when accessing either EACMS or PACS.	2018
CIP-002-5.1a	Requirement R1	Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets.	2023
CIP-002-5.1a	Requirement R1	Enhance policies and procedures to include evaluation of Cyber Asset misuse and degradation during asset categorization.	2021
CIP-002-5.1a	Requirement R1	Ensure that all BES Cyber Assets are properly identified.	2020

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-002-5.1a	Requirement R1 Attachment 1 Criterion 2.5	Ensure that all substation BES Cyber Systems are properly categorized as high, medium, or low impact.	2020
CIP-002-5.1a	Requirements R1 Attachment 1 Criterion 2.8	Consider all generation assets, regardless of ownership, when categorizing BES Cyber Systems associated with transmission facilities.	2019
CIP-002-5.1a	Requirement R1	Consider all owned generation assets, regardless of BES-classification, when evaluating impact ratings to ensure proper classification of BES Cyber Systems.	2017
CIP-002-5.1a	Requirement R1	Identify and categorize cyber systems used for supporting generation, in addition to the cyber systems used to directly control generation.	2017
CIP-002-5.1a	Requirement R1	Ensure that all shared facility categorizations are coordinated between the owners of the shared facility through clearly defined and documented responsibilities for CIP Reliability Standards compliance.	2017
CIP-003-8 CIP-007-6 CIP-008-6	Requirement R2, Section 4 Requirement R4 Requirement R4	Ensure reportable Cyber Security Incidents and attempts to compromise that were identified as Cyber Security Incidents are reported to Electricity Information Sharing and Analysis Center (E-ISAC) and Cybersecurity and Infrastructure Security Agency (CISA).	2023
CIP-003-8	Requirement R2	Re-evaluate policies, procedures, and controls for Low-impact Cyber Systems and associated Cyber Assets.	2022

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-003-8	Requirement R2, Attachment 1, Section 5.2.1	Properly document and implement policies, procedures, and controls for low impact TCAs.	2021
CIP-004-6	Requirement R4	Implement a defined workflow to enhance processes for the verification of electronic access, unescorted physical access, and access to BES Cyber System Information (BCSI).	2021
CIP-004-6	Requirement R4.1.3	Base access to BCSI on "need to know."	2021
CIP-004-6	Requirements R4 and R5	Ensure that access to BES Cyber System Information (BCSI) is properly authorized and revoked.	2020
CIP-004-6	Requirement R2	Ensure that all employees and third-party contractors complete the required training and that the training records are properly maintained.	2019
CIP-004-6	Requirement R4	Verify employees' recurring authorizations for using removable media.	2019
CIP-004-6	Table R1 Security Awareness Program	Enhance documented processes and procedures for security awareness training to consider NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program" guidance.	2018
CIP-004-6	Requirement R3	Conduct a detailed review of contractor personnel risk assessment processes to ensure sufficiency and to address any gaps.	2017

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-004-6	Requirement R4	Conduct a detailed review of physical key management to ensure the same rigor in policies and testing procedures used for electronic access is applied to physical keys used to access the physical security perimeter	2017
CIP-004-6	Requirement R4	Enhance procedures, testing, and controls around manual transfer of access rights between personnel accessing tracking systems, PACS, and Electronic Access EACMS or, alternatively, consider the use of automated access rights provisioning.	2017
CIP-004-6	Requirement R4	Ensure that access permissions within personnel access tracking systems are clearly mapped to the associated access rights within PACS and EACMS.	2017
CIP-005-7	Requirement R1.3	Restrict all inbound and outbound access permissions, including the reason for granting access and denying all other access by default.	2023
CIP-005-5	Requirement R1	Review all firewalls to ensure there are no obsolete or overly permissive firewall access control rules in use.	2019
CIP-005-5	Requirement R2	Consider implementing encryption for Interactive Remote Access (IRA) that is sufficiently strong to protect the data that is sent between the remote access client and the BES Cyber System's Intermediate System.	2018
CIP-005-5	Requirement R1	Ensure that policies and testing procedures for all electronic communications protocols are afforded the same rigor.	2017
CIP-005-5	Requirement R1	Perform regular physical inspections of BES Cyber Systems to ensure no unidentified EAPs exist.	2017

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-005-5	Requirement R1	Review all firewall rules and ensure access control lists follow the principle of "least privilege."	2017
CIP-005-5	Requirement R2	For each remote cyber asset conducting Interactive Remote Access (IRA), disable all other network access outside of the connection to the BES Cyber System that is being remotely accessed, unless there is a documented business or operational need.	2017
CIP-005-5 and CIP-007-6	Requirement R1 and R5	Consider implementing valid Security Certificates within the boundaries of BES Cyber Systems with encryption sufficiently strong to ensure proper authentication of internal connections.	2018
CIP-006-6	Requirement R1	Consider having a dedicated visitor log at each physical security perimeter access point.	2020
CIP-006-6	Requirement R1	Consider locking BES Cyber Systems' server racks where possible.	2020
CIP-006-6	Requirement R1	Inspect all physical security perimeters periodically to ensure that no unidentified physical access points exist.	2020
CIP-006-6	Requirement R1	Limit access to employee's personal identification numbers used for accessing physical security perimeters using a least-privilege approach.	2019
CIP-006-6	Requirement R2	Enhance processes and controls around the use of manual logs, such as using highly visible instructions outlining all the parts of the requirement with each manual log, to consistently capture all required information.	2017

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-007-6	Requirement R1	Ensure physical and logical port protection controls for Cyber Assets.	2021
CIP-007-6 & CIP-010-4	Requirement R2.3 & Requirement 3.4	Address risks posed by BES Cyber Assets that have reached the manufacturer-determined end of life/service and are no longer supported by vendors.	2022
CIP-007-6	Requirement R3	Deploy a comprehensive malicious code prevention program for all Cyber Assets within a BES Cyber System.	2022
CIP-007-6	Requirement R5	Review the system access control program periodically to ensure processes and procedures are implemented as documented.	2021
CIP-007-6	Requirement R2	Review security patch management processes periodically and ensure that they are implemented properly.	2020
CIP-007-6	Requirement R5	Consider consolidating and centralizing password change procedures and documentation.	2020
CIP-007-6	Requirement R1	Ensure that all ephemeral port ranges are within the Internet Assigned Numbers Authority (IANA) recommended ranges.	2019
CIP-007-6	Requirement R1	Consider Internet Control Message Protocol (ICMP) as a logical access port for all the BES Cyber Assets.	2018
CIP-007-6	Requirement R2	Consider incorporating file verification methods, such as hashing, during manual patching processes and procedures, where appropriate.	2018

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-007-6	Requirement R1	Enhance processes and procedures for documenting the determination for each cyber asset that has no provision for disabling or restricting ports, to ensure consistency and detail in the documentation.	2017
CIP-007-6	Requirement R3	Consider employing host-based malicious code prevention for all cyber assets within a BES Cyber System, in addition to network level prevention, for non-Windows based cyber assets as well as Windows-based cyber assets.	2017
CIP-007-6	Requirement R5	Implement procedures and controls to monitor or limit the number of simultaneously successful logins to multiple different systems.	2017
CIP-007-6 and CIP-010-2	Requirement R2 and R1	Consider replacing or upgrading "End-of-Life" system components of an applicable Cyber Asset.	2018
CIP-008-5	Incident Reporting and Response Planning	Enhance documented processes and procedures for incident response to consider the NIST SP 800-61, "Computer Security Incident Handling Guide."	2018
CIP-009-2	Requirement R2	Enhance recovery and testing plans to include a sample of any offsite backup images in the representative sample of data used to test the restoration of BES Cyber Systems.	2021
CIP-009-6	Requirement R1	Ensure that backup and recovery procedures are updated in a timely manner.	2020
CIP-010-2	Requirement R3	Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.	2020
CIP-010-2	Requirement R4	Clearly mark TCAs and Removable Media.	2019

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-010-2	Requirement R3	Consider the remote configuration of applicable Cyber Assets via a TCP/IP-to-RS232 Bridge during vulnerability assessments.	2018
CIP-010-2	Table R2 Configuration Monitoring	Consider using automated mechanisms that enforce asset inventory updates during configuration management.	2018
CIP-010-2	Requirement R2	Implement procedures to detect and investigate unauthorized changes to baseline configurations.	2017
CIP-010-3	Requirement R1	Review configuration change management processes periodically and ensure that they are implemented properly.	2021
CIP-010-3	Requirement R1.5	Enhance configuration change management procedures and controls to document and account for differences between test and production environments.	2021
CIP-010-3	Requirement R3	Improve vulnerability assessments to include credential-based scans of Cyber Assets.	2021
CIP-010-3	Requirement R4	Properly document and implement policies, procedures, and controls for medium and high impact TCAs.	2021
CIP-010-4	Requirement R3	Implement comprehensive vulnerability assessment processes for applicable Cyber Assets.	2022
CIP-010-4	Requirement R4	Review and validate controls used to mitigate software vulnerabilities and malicious code on Transient Cyber Assets (TCAs) managed by a third party. TCAs are generally portable electronic devices used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	2022

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-011-2	Requirement R1.2	Enhance policies and procedures to include BCSI spillage investigation and response.	2021
CIP-011-2	Requirement R1.1.2	Enhance policies, procedures, and controls to properly track, document and monitor BCSI storage locations.	2021
CIP-011-2	Requirement R2	Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.	2020
CIP-011-2	Requirement R1	Ensure that all commercially available enterprise software tools are included in BSCI storage evaluation procedures.	2017
CIP-011-2	Requirement R1	Enhance documented processes and procedures for identifying BCSI to consider the NERC Critical Infrastructure Protection Committee (CIPC) guidance document, "Security Guideline for the Electricity Sector: Protecting Sensitive Information."	2017
CIP-011-2	Requirement R1	Document all procedures for the proper handling of BCSI.	2017
CIP-011-2	Requirement R1.2	Ensure that all the security controls implemented by third parties are evaluated regularly and implement additional controls where needed when using a third party to manage BES Cyber System Information (BCSI).	2020
CIP-013-1	Requirement R1	Enhance supply chain risk management programs to include evaluating the supply chain risks of existing vendors and develop a plan to respond to the risks that are identified.	2023

FEDERAL ENERGY REGULATORY COMMISSION
Office of Electric Reliability
Division of Cyber Security

FERC.GOV