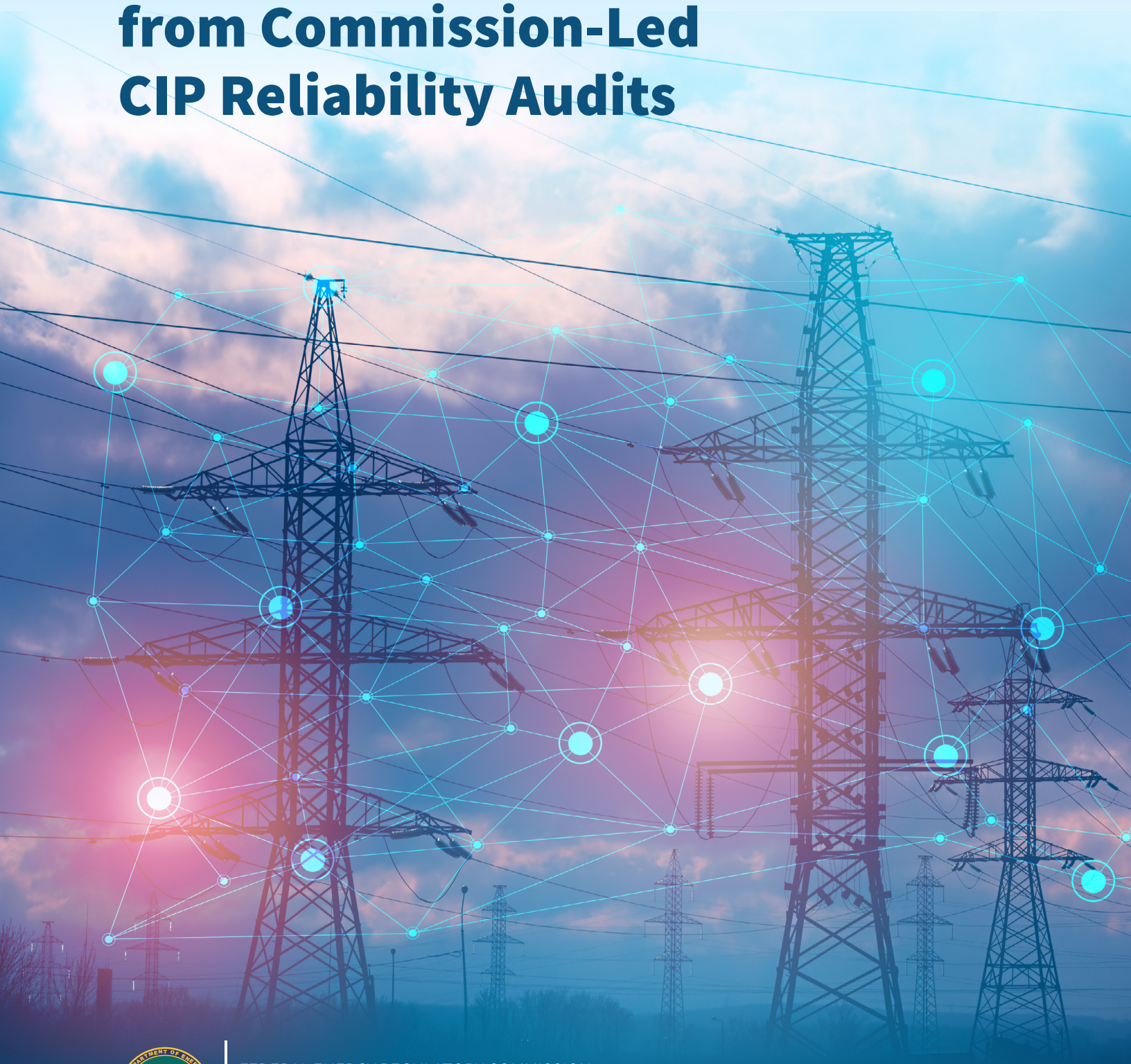
2023
Lessons Learned from Commission-Led CIP Reliability Audits



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

2023
Lessons Learned from Commission-Led CIP Reliability Audits

A Staff Report

December 11, 2023

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

TABLE OF CONTENTS

INTRODUCTION

During Fiscal Year (FY) 2023,[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 FY2023 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 BES.

1 The fiscal year is the accounting period for the federal government which begins on October 1st and ends on September 30th. The fiscal year is designated by the calendar year in which it ends; for example, FY2023 begins on October 1, 2022 and ends on September 30, 2023.

2 Section 215 to the Federal Power Act (FPA) gives NERC (as the Commission-approved Electric Reliability Organization (ERO)) the authority to establish and enforce Reliability Standards, which are subject to Commission review and approval. 16 U.S.C. § 824o. NERC uses the Commission-approved term Bulk Electric System (BES) definition, a subset of the Bulk-Power System, to define the scope of the Reliability Standards and to register a subset of Bulk-Power System users, owners, and operators subject to the mandatory and enforceable Reliability Standards. *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012) , order on reh'g, Order No. 773A, 143 FERC ¶ 61,053 (2013) rev'd sub nom. People of the State of New York v. FERC, 783 F.3d 946 (2d Cir. 2015); NERC, Glossary of Terms Used in NERC Reliability Standards, 5-7 (Mar. 29, 2022), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (NERC Glossary).

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 the CIP Reliability audits. However, the Office of Electric Reliability consulted with OEIS regarding the voluntary practices observed by staff during the CIP audits that are discussed in this report. OEIS is not responsible for the development or enforcement of CIP Standards but instead is responsible for the identification and implementation 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.

CIP RELIABILITY STANDARDS

Section 215 of the Federal Power Act (FPA) provides that the Commission may certify an Electric Reliability Organization (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.[5] The Commission established a process to select and certify an ERO,[6] and subsequently certified NERC.[7]

The CIP Standards are designed to mitigate the cyber security and physical security risks to BES facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result 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.[8] 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.[9]

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-003-8 – Cyber Security - Security Management Controls
3. CIP-005-7 – Cyber Security — Electronic Security Perimeter(s)
4. CIP-007-6 – Cyber Security – System Security Management
5. CIP-008-6 – Cyber Security - Incident Reporting and Response Planning
6. CIP-010-4 - Cyber Security - Configuration Change Management and Vulnerability
7. CIP-013-2 – Cyber Security - Supply Chain Risk Management

5 16 U.S.C. § 824o.

6 *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, order on reh'g, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

7 *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).

8 *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).

9 *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 primarily consisted of data requests and reviews, webinars and teleconferences, and virtual and on-site interview sessions. Prior to the interview sessions, 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 interview sessions, staff interviewed the entities' subject matter experts and observed demonstrations of operating practices, processes, and procedures used by the entities' personnel. Additionally, staff interviewed employees and managers responsible for performing tasks within the audit scope and analyzed documentation to verify compliance with requirements; conducted several field inspections remotely and observed the functioning of applicable Cyber Assets[10] identified by the registered entity as High, Medium, or Low Impact;[11] and interviewed compliance program managers, staff, and employees responsible for day-to-day compliance and regulatory oversight. Applicable Cyber Assets consisted of BES Cyber Assets[12] and Protected Cyber Assets[13] within a BES Cyber System[14] or associated Cyber Assets mainly, but not always, outside the BES Cyber System (i.e., Electronic Access Control or Monitoring Systems (EACMS)[15] and Physical Access Control Systems (PACS)).[16]

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.

10 The NERC Glossary defines "Cyber Assets" as programmable electronic devices, including the hardware, software, and data in those devices.

11 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.

12 The NERC Glossary defines "BES Cyber Asset" as 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.

13 The NERC Glossary defines "Protected Cyber Asset" as a Cyber Asset connected using a routable protocol within or on an Electronic Security Perimeter (ESP) that is 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.

14 The NERC Glossary defines "BES Cyber System" One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

15 The NERC Glossary defines "Electronic Access Control or Monitoring Systems" (EACMS) as Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

16 The NERC Glossary defines "Physical Access Control Systems" (PACS) as Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

OVERVIEW OF LESSONS LEARNED

The lessons discussed in this report are intended to help registered entities improve their compliance with the CIP Standards and their overall cyber security posture. The lessons learned are presented in order by CIP Standard:

Lessons Learned	*Relevant CIP Standard(s)*
1. Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets.	CIP-002-5.1a, R1
2. 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).	CIP-003-8, R2, Section 4 CIP-007-6, R4 CIP-008-6, R4
3. Restrict all inbound and outbound access permissions, including the reason for granting access and denying all other access by default.	CIP-005-7, R1.3
4. 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.	CIP-013-1, R1

LESSONS LEARNED DISCUSSION

BES Cyber System Asset Identification and Categorization

CIP-002-5.1A, REQUIREMENT R1

Overview

Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets. 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 BES. 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. Identification and categorization of BES Cyber Systems supports appropriate protection against compromises that could lead to mis-operation or instability in the BES.

Of relevance to the discussion below, Reliability Standard CIP-002-5.1a Attachment 1, Criteria 2.6 categorizes as medium impact "Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Background

During Commission-led CIP audits conducted during FY 2022-2023, audit staff found that while entities generally had strong processes and procedures for the identification of their BES Cyber Systems, in some cases BES Cyber Systems were not identified and categorized properly. Specifically, audit staff identified the following two circumstances in which entities failed to properly identify and categorize BES Cyber Systems:

1. Some entities did not identify each medium impact BES Cyber System at a single plant location identified by a Reliability Coordinator as critical to the derivation of IROLs and their associated contingencies, as required by Attachment 1, Section 2.6. In particular, some entities limited their identification and categorization to a specific BES Cyber System instead of considering their entire facility as being critical, per the requirement language.
2. Entities that deployed hypervisors within their network environment did not accurately identify and categorize all BES Cyber Systems based on the highest impact level of the virtual assets that they manage.[17] Entities adopting virtualization technologies typically separate the hypervisor host and the virtual machines. As a consequence of this separation, some entities only identified the virtual machines (as EACMS, PCAs, or BES Cyber Assets), but did not identify the hypervisor used to host and store configuration files of the virtual machines.[18] In

17 A hypervisor is the software used to operate virtual machines, allowing one physical Cyber Asset to host multiple virtual machines by sharing hardware resources, such as memory and processing. An entity may use a hypervisor to manage assets in their corporate environment, OT environment, or a mixed environment, where one hypervisor operates assets in both environments.

18 A virtual machine is the software representation of a physical device consisting of virtualized hardware, operating system (guest OS), and applications.

some instances, key hardware resources and processes associated with the hypervisors were not identified and thus not given the same classification as the parent hypervisor.

Risk

The identification and categorization of BES Cyber Systems forms the foundation of the CIP Reliability Standards. Miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate cyber security controls, or no controls at all. This weakened cybersecurity posture can lead to compromise or misuse that can ultimately affect the real-time operation of the BES.

BES Cyber System Asset Identification and Categorization Filed Violations (2017 - 2021)

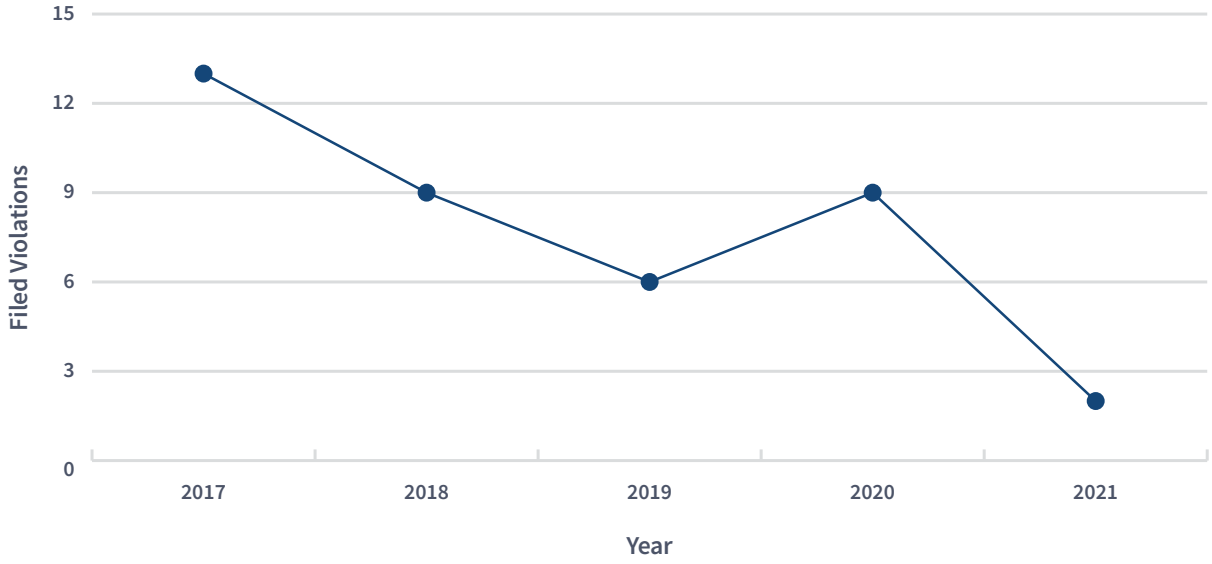


Figure 1. During the period of 2017 through 2021, 39 violations related to CIP-002-5.1a Requirement R1 were filed with the Commission. While these findings have trended downward since 2017, the security risks remain.

Mitigations

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

1. When informed by a Reliability Coordinator, Planning Coordinator, or Transmission Planner that a generation plant or transmission facility is critical to the derivation of IROLs and their associated contingencies, some entities did not apply the medium impact categorization to the entire plant or facility as required by Reliability Standard CIP-002-5.1a, Attachment 1, Criteria 2.6. An entity's identification and categorization procedure should recognize any shared processes and subsequent control networks the facility may have that could impact its critical function(s). For example, if an entity has identified voltage regulation as critical to the derivation of IROLs as set forth in criteria 2.6, the entity must consider the associated generation and subsequent control networks as medium impact BES Cyber Systems.
2. Entities that deploy hypervisors in their networks environments including those being used in mixed environments, categorize the hypervisor at the highest impact level of the asset(s) the hypervisor manages,

including its shared resources and processes. For example, if a hypervisor manages several assets including a medium impact PCA, the entity must also identify the hypervisor as a medium impact BES Cyber System. Additionally, the hypervisor in its entirety must receive that classification. Any shared resources, processes, or data used by the hypervisor must also be categorized as medium impact, even if located outside an entity's ESP.

Additional Guidance

NERC *ERO ENTERPRISE CMEP PRACTICE GUIDE: ASSESSMENT OF VIRTUALIZED SYSTEMS*

https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20%20Virtual%20Systems.pdf

NOTE: See section Assessment of Virtualized Systems and pages 1-5.

NIST *SP 800-125A REV. 1: SECURITY RECOMMENDATIONS FOR SERVER-BASED HYPERVISOR PLATFORMS*

https://csrc.nist.gov/pubs/sp/800/125/a/r1/final

NOTE: See section Approach for Developing Security Recommendations and pages 12-39.

Cyber Security Incident Notification

CIP-003-8, REQUIREMENT R2, ATTACHMENT 1, SECTION 4
CIP-007-6, REQUIREMENT R4,
CIP-008-6, REQUIREMENT R4

Overview

Ensure Reportable Cyber Security Incidents and attempts to compromise that were identified as Cyber Security Incidents are reported to E-ISAC and CISA. Reliability Standard CIP-008-6, Requirement R4 requires entities with medium and high impact BES Cyber Systems and associated EACMS to notify the NERC Electricity Information Sharing and Analysis Center (E-ISAC) and Cybersecurity and Infrastructure Security Agency (CISA)[19] of a "Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise," based on the application of criteria set forth in the Reliability Standard.[20]

A separate requirement obligates the reporting of Reportable Cyber Security Incidents for assets containing low impact BES Cyber Systems. Specifically, pursuant to CIP-003-8, Requirement 2, Attachment 1, Section 4, entities must determine whether an identified Cyber Security Incident occurring at an asset containing a low impact BES Cyber System is a Reportable Cyber Security Incident and subsequently notify the E-ISAC, unless prohibited by law. Unique to Low Impact BES Cyber Systems, the Reportable Cyber Security Incident must have "compromised or disrupted: A BES Cyber System that performs one or more reliability tasks of a functional entity."[21]

Background

Required notifications provide the E-ISAC (CIP-008-6 and CIP-003-8) and CISA (CIP-008-6) with the opportunity to analyze the incidents or threats and, when warranted, warn other entities of the incidents or threats. Such alerts or bulletins issued from E-ISAC or CISA Central[22] typically broadcast generalized threat information without identifying the reporting entity. The information broadcasted by E-ISAC and/or CISA Central informs electric industry stakeholders regarding the effectiveness of security controls that apply to BES Cyber Systems and critical energy infrastructure. Entities then have the opportunity to take appropriate responsive action to mitigate the known threat. Thus, the reporting process contributes to the overall improvement of the cybersecurity posture of the BES.

Throughout Commission-led audits conducted during FY2022-2023, audit staff found that entities generally documented both (i) processes to identify, classify, and respond to Cyber Security Incidents, and (ii) criteria to evaluate and define a Reportable Cyber Security Incident and an attempt to compromise. However, in some instances, entities did not submit required Cyber Security Incidents reports to the E-ISAC and/or CISA in accordance with the entity's documented processes and criteria required by CIP-008-6 and CIP-003-8.

---

19 CISA is the successor to the United States National Cybersecurity and Communications Integration Center (NCCIC) pursuant to CIP-008-6, where medium and high impact entities are required to report to both E-ISAC and CISA for Cyber Security Incident reporting.

20 *See* NERC Glossary definition of Cyber Security Incident for additional details.

21 *See* NERC Glossary definition of Reportable Cyber Security Incident for additional details. *See also* Reliability Standard CIP-003-8, Supplemental Material, at 50-51.

22 CISA's 24x7x365 operations center is called CISA Central, and it provides situational awareness and near-real time operational reporting on events impacting the nation's 16 critical infrastructure sectors. *See* https://www.cisa.gov/cisa-central.

The following examples illustrate circumstances in which entities did not identify Cyber Security Incidents, including unauthorized malware that was verified as malicious. As a result, the entities did not report to the E-ISAC and CISA (CIP-008-6 only) as they were required.

1. **Inadequate documented processes:** An entity did not include potential security events logged or alerted, required by Reliability Standard CIP-007-6, Requirement R4,[23] as a compromise or attempt to compromise within the entity's Cyber Security Incident Response Plan. The entity's Cyber Security Incident Response Plan was not activated when malware was found in logs and was not reported as required. The entity should have included logged and alerted security events in its CIP-007-6 and CIP-008-6 plans, noting that logs and alerts could activate the Cyber Security Incident Response Plan and lead to a Cyber Security Incident that required reporting, per CIP-008-6 Requirement 1.
2. **Documented plan not followed:** An entity discovered malware identified by its antivirus solution on a BES Cyber System. While this type of event was included in the entity's Cyber Security Incident Response Plan the entity determined regardless of its Plan that it was not compromised because the BES Cyber System was isolated and was unable to communicate to the malware's command-and-control server. The entity should have followed its documented Plan and reported the malware to E-ISAC and CISA, consistent with CIP-008-6 Requirements 1 & 4.
3. **Unreported identified malware – Scenario 1:** An entity found malicious code on an installer recognized by its antivirus solution, but the installer was in the BES Cyber System's recycle bin and required human interaction to activate the malware. The entity determined that the system was not compromised based on (i) the location of the malicious code and (ii) the situation was not addressed in the entity's Cyber Security Incident Response Plan. The discovered malware, however, was unauthorized code with the potential to perform malicious actions. The entity should have reported the malicious code that existed on its BES Cyber System, regardless of the location, consistent with CIP-008-6 Requirements 1 & 4.
4. **Unreported identified malware – Scenario 2:** An entity identified malware on its Low Impact BES Cyber System and determined that, because the system continued operating, it was not obligated to report the incident. The malware in question was part of a major malware campaign and the entity only identified the malicious traffic from the malware due to the guidance from a NERC Alert and CISA publication. The entity errantly claimed that the event was not reportable because there was no associated outage. In fact, the entity should have identified the malware as a Reportable Cyber Security Incident since it was "a Cyber Security Incident that compromised a BES Cyber System that performed one or more reliability tasks of a functional entity," consistent with Reliability Standard CIP-003-8 Requirement 2, Attachment 1, Section 4.[24]

Risk

Unreported Cyber Security Incidents can cause incomplete or inaccurate risk evaluations for entities and the BES due to improper identification and assessment of compromises and attempts to compromise. And these incomplete or inaccurate risk evaluations may lead to malicious acts and suspicious events being assessed a likelihood and/or an

23 Reliability Standard CIP-007-6 Requirement 4, Part 4.1: "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code. Part 4.4: "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

24 Reliability Standard CIP-003-8 Requirement R2, Attachment 1, Section 4, Part 4.2 states: "Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include: 4.1 Identification, classification, and response to Cyber Security Incidents; 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law."

impact rating that is not reflective of the actual threat posed to the entity and the BES, or risks may go unidentified entirely. Incidents that could be indicators of a broader malware campaign could go unreported and result in a lack of situational awareness for BES entities, and they may not take actions to mitigate Cyber Security Incidents. Failure to categorize incidents properly may also lead to complacency with respect to identification and response.

Cyber Security Incident Reporting Filed Violations (2017 - 2021)

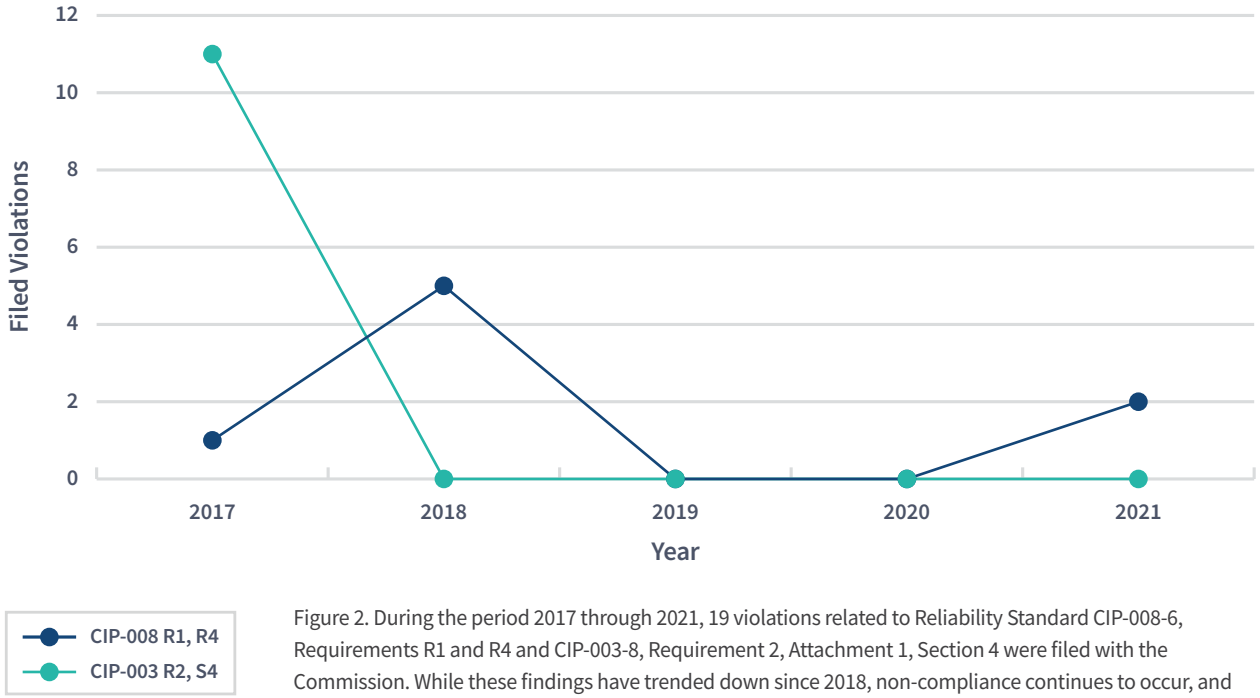


Figure 2. During the period 2017 through 2021, 19 violations related to Reliability Standard CIP-008-6, Requirements R1 and R4 and CIP-003-8, Requirement 2, Attachment 1, Section 4 were filed with the Commission. While these findings have trended down since 2018, non-compliance continues to occur, and the security risks remain.

Mitigations

Entities should consider multiple mitigations within the CIP Reliability Standards to enhance accurate reporting of Cyber Security Incidents.

1. **Cyber Security Incident Response Plan: CIP-008-6 Requirement R1 and CIP-003-8, Requirement R2, Attachment 1, Section 4:** Enhance Cyber Incident Response Plans by developing more holistic criteria for the identification of Cyber Security Incidents, including addressing realistic and most likely scenarios, roles and responsibilities, logistics, and chain of communication, as well as addressing how these details could change based on differing scenarios. This will provide additional guidance for team members during an actual Cyber Security Incident.
2. **Security Event Logging and Alerting: CIP-007-6 Requirement R4:** Enhance alert processing and investigation of CIP-related security events. In particular, refine processes for distinguishing and prioritizing CIP-related event logs from non-BES Cyber System event logs, such as updating CIP related event alert parameters.
3. **Removable Media: CIP-010-4, Requirement R4 and CIP-003-8, Requirement R2, Attachment 1, Section 5:** These Reliability Standards require the protection of Low, Medium and high impact BES Cyber Assets from vulnerabilities introduced by removable media such as floppy disks, compact disks, USB flash drives, and

external hard drives.[25] Robust procedures and controls pertaining to removable media, in addition to those explicitly identified in the above Reliability Standards, will enhance prevention and mitigation of Cyber Security Incidents. In particular, entities should consider implementing additional procedures and controls to track and log removable media even when not in use. Further, entities should retain results from scans of removable media for an appropriate amount of time in order to trace malware in case an incident occurs.

Additional Guidance

NIST *SP 800-61 REVISION 2: COMPUTER SECURITY INCIDENT HANDLING GUIDE*

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NOTE: see sections #2 Organizing a Computer Security Incident Response, and #3 Handling an Incident.

NIST *SP 800-82 REVISION 3: GUIDE TO OPERATIONAL TECHNOLOGY (OT) SECURITY*

https://csrc.nist.gov/News/2023/nist-publishes-sp-800-82-revision-3

NOTE: see sections (3.3.8) Develop an Incident Response Capability, (6.2.4.5) Response and Recovery Plans (PR. IP-9) and Response and Recovery Plan Testing (PR.IP-10), (6.3) Applying the Cybersecurity Framework to OT: Detect (including Anomalies and Events, Security Continuous Monitoring, and Detection Process), (6.4) Applying the Cybersecurity Framework to OT: Response, Appendix C: Threat Sources, Vulnerabilities, and Incidents, Appendix E: OT Security Capabilities and Tools, and Appendix F: OT Overlay F.7.8. INCIDENT RESPONSE – IR.

25 *See* NERC Glossary definition of Removable Media for additional details.

CIP Reliability Standards Low Impact Cyber Security Incident Reporting (CIP-003-8)

Standard	What to Report	Where to Report	Reporting Options	Notes
CIP-003-8 (Low Impact)	Reportable Cyber Security Incident	E-ISAC	**E-ISAC Portal:** https://www.eisac.com/s/ **E-ISAC Email:** operations@eisac.com **E-ISAC Phone:** 202-790-6000 **DOE-OE-417 Form:** https://www.oe.netl.doe.gov/oe417.aspx	The E-ISAC Portal offers online submission with a Portal account. DOE OE-417 Form provides the option to notify one or a combination of: (1) NERC, (2) E-ISAC, and (3) CISA Central. The Form is available for online submission or email. NERC EOP-004 reporting can be used in some cases. https://www.nerc.com/pa/Stand/Reliability Standards/EOP-004-4.pdf

CIP Reliability Standards Medium & High Impact Cyber Security Incident Reporting (CIP-008-6)

Standard	What to Report	Where to Report	Reporting Options	Notes
CIP-008-6 (Medium and High Impact)	Reportable Cyber Security Incident & Cyber Security Incident that was an attempt to compromise	E-ISAC	**E-ISAC Portal:** https://www.eisac.com/s/ **E-ISAC Email:** operations@eisac.com **E-ISAC Phone:** 202-790-6000 **DOE-OE-417 Form:** https://www.oe.netl.doe.gov/oe417.aspx	Entities must report to both E-ISAC and CISA Central. E-ISAC Portal offers online submission with a Portal account. Email and phone are also available. DOE OE-417 Form provides the option to notify one or a combination of: (1) NERC, (2) E-ISAC, and/or (3) CISA Central. The Form is available for online submission or to be emailed. NERC EOP-004 reporting can be used in some cases. https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-4.pdf
		CISA Central	**Email:** report@cisa.gov **Phone:** (888) 282-0870 **DOE-OE-417 Form** https://www.oe.netl.doe.gov/oe417.aspx	https://www.cisa.gov/cisa-central DOE OE-417 Form provides the option to notify one or a combination of: (1) NERC, (2) E-ISAC, and/or (3) CISA Central. The Form is available for online submission or to be emailed.

Electronic Security Perimeter Inbound and Outbound Access

CIP-005-7, REQUIREMENT R1.3

Overview

Restrict all inbound and outbound access permissions, including the reason for granting access, and denying all other access by default. Reliability Standard CIP-005-7, Requirement R1 states that each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-7 Table R1 – Electronic Security Perimeter (ESP). Requirement R1.1.3 requires inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-005-7 Table R1 – Electronic Security Perimeter and additional evidence to demonstrate implementation as described in the Measures column of the table.

Background

During Commission-led CIP audits conducted during FY 2022-2023, audit staff found that while entities generally restricted inbound and outbound access permissions at electronic access points (EAP), in some cases entities did not restrict inbound and outbound access permissions and /or document the reason for granting access. In multiple instances, audit staff noted that one or both elements were not performed by the entity.

For example, some entities allowed Internet Control Message Protocol[26] traffic of all types through electronic access points in its primary and back-up control center ESPs without documenting its use or the reason for its use. Audit staff noted instances in which BES Cyber Assets could "ping" an internet address outside an entity's primary and back-up control center ESPs. In most cases, entities did not document the use of Internet Control Message Protocol and the reason for its use throughout the network. In addition to Internet Control Message Protocol communications, audit staff noted that some entities did not have documented justifications for inbound and outbound communications through electronic access points. In other instances, audit staff observed that entities maintained overly permissive access permissions at electronic access points, to include the use of ranges outside those required by applicable Cyber Assets, and failing to deny all other unnecessary traffic by default.

Risk

Allowing the use of protocols such as ICMP throughout the network without valid reason and oversight could lead to possible security compromise, such as Ping of Death[27] or distributed denial of service attacks.[28] EAPs must have all inbound and outbound traffic justified[29] because EAPs are a common vector of attack. Not properly accounting for all traffic could lead to compromise and/or mis-operation of BES Cyber Systems. If Cyber Assets within the ESP become

26 Internet Control Message Protocol or "ICMP" is a supporting protocol of the Internet protocol suite used primarily to deliver error messages to Internet Protocol users and to perform network diagnostics. Internet Control Message Protocol has many messages that are identified by a "type" field. Some important and widely used messages include Echo Reply, Echo Request, Redirect, Destination Unreachable, Traceroute, and Time Exceeded.

27 Ping of Death is a type of denial of service attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

28 A distributed denial of service attack attempts to disrupt normal traffic of a server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic by utilizing multiple compromised computer systems as sources of attack traffic.

29 CIP-005-7 – Cyber Security — Electronic Security Perimeter(s) Requirements 1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

compromised and attempt to communicate to unknown hosts outside the ESP (usually "command and control" hosts on the Internet or compromised "Intermediate System" within the entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit.

Inbound and Outbound Access Filed Violations (2017 - 2021)

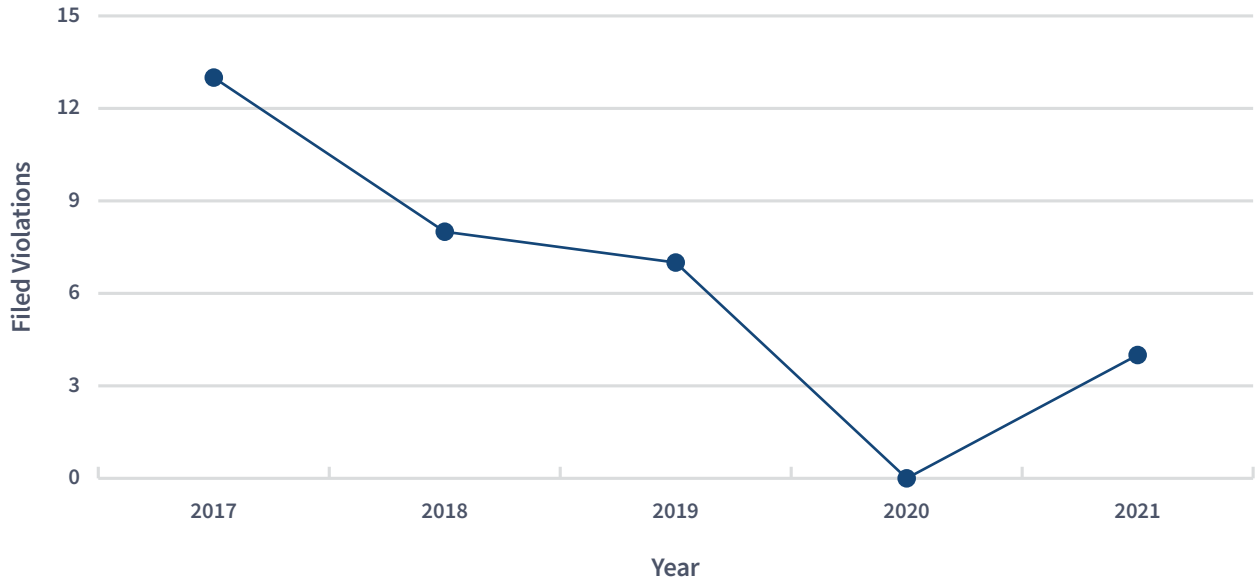


Figure 3. During the period of 2017 through 2021, 32 violations related to CIP-005-7 Requirement 1 were filed with the Commission. These findings have trended downward since 2017, but security risks remain.

Mitigations

Entities should consider multiple mitigations to enhance electronic access control:

1. Entities should ensure all inbound and outbound access permissions are accounted for, including documenting the reason for granting access and denying all other access by default.
2. Entities should review EAP configurations on a quarterly basis to ensure access permissions are documented and all other access is denied by default.
3. Best practice for entities that have not yet deployed Internet Protocol Version Six (IPv6)[30] to communicate outside the protected environment is to block all IPv6 at the network border, including any IPv6 that is tunneled into IPv4. If IPv6 is deployed, in a dual stack (IPv4 and IPv6 concurrently) configuration, ensure corresponding security controls are implemented for IPv6, addressing any specific differences in the new protocol. Default or misconfigured IPv6-enabled devices could introduce vulnerabilities, making the devices more prone to compromise. Ensure intrusion sensors and logs related to IPv6 traffic are ingested and reviewed in a corresponding manner as IPv4.

30 IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4). One of the primary needs for this is to expand the number of available addresses which is running out in IPv4. (Source: https://www.rfc-editor.org/rfc/rfc2460.html)

Additional Guidance

NIST *SP-800-41 GUIDELINES ON FIREWALLS AND FIREWALL POLICY*

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

NOTE: See section 4 and pages 4-1 through 4-7

NIST, DHS, CISA *RECOMMENDED PRACTICE: IMPROVING INDUSTRIAL CONTROL SYSTEM CYBERSECURITY WITH DEFENSE-IN-DEPTH STRATEGIES*

https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

NOTE: See section 2.5.2 and pages 23-24

NSA IPV6 SECURITY GUIDANCE

https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/1/CSI_IPv6_security_guidance_.PDF

Supply Chain Risk Management

CIP-013-1, REQUIREMENT R1

Overview

Enhance the entity's supply chain risk management program to include (i) evaluating the supply chain risks of existing vendors and (ii) developing a plan to respond to identified vendor-related risks. Reliability Standard CIP-013-1, Requirement R1 requires entities to develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. Pursuant to Requirement R1.3, the plan(s) must include one or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

While the requirement language obligates entities to develop a supply chain risk management plan with various characteristics, it does not mandate that the plan apply to contracts that were in effect at the effective date of the Reliability Standard. Additionally, the standard does not require the plan to incorporate responses to the risks identified by the entity in the plan except in limited circumstances (Requirement Part 1.4.2). Throughout the course of audit fieldwork, audit staff has identified these areas as representing best practices that entities should seek to implement to enhance the robustness of their supply chain risk management programs.

Background

During Commission-led CIP audits conducted during FY 2022-2023, audit staff found that while entities generally maintained supply chain risk management plans to assess cyber risks associated with new vendors contracted after the enforcement date of Reliability Standard CIP-013-1 (October 1, 2020), in some cases they did not develop risk responses to the risks that were identified. While not required by the Standard, audit staff noticed disparities in the understanding that entities had of their risk exposure from existing contracts and vendor relationships that were not fully considered by their supply chain risk management plans, versus those that had complete risk assessments under the parameters required by the criteria in CIP-013-1. This disparity resulted in entities not having a definitive strategy regarding how they would respond to various risk events posed by potential issues that may arise from existing contracts.

Risk

Since the effective enforcement date of October 1, 2020, audit staff has made one audit finding related to Reliability Standard CIP-013-1, Requirement R1. However, given the recent effective date of the supply chain standard and emerging supply chain risks, the number of audit findings is not indicative of risk mitigation in the electric industry.

Audit staff observed that some entities lacked consistency and effectiveness when evaluating vendors and procuring vendor-supplied equipment and software. Some audited entities had incorporated strong vendor risk evaluation processes into their enterprise-wide risk management programs and displayed a consistent application of the risk identification assessment process to each of their vendors. However, audit staff observed that other audited entities' supply chain risk identification and assessment processes were unclear and generally lacked rigor. Staff also observed multiple instances where entities failed to properly implement their own supply chain risk management plans. In some cases, staff found that entities' supply chain risk management plans did not include processes or

procedures to respond to risks once identified, specifically for "grandfathered' contracts that existed prior to the effective date of the Reliability Standard. In some circumstances where these contracts were considered in the risk management plans, there was minimal consideration given to mitigation and response strategies. Audit staff recommends that entities include responses to every risk event identified in their supply chain risk management plans to ensure that appropriate mitigations are employed such that the entity has no "blind spots" in its operations.

While entities are not required by Reliability Standard CIP-013-1 to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), entities should consider applying their supply chain risk management plans to their existing vendors to ensure that they are appropriately identifying and addressing supply chain risks applicable to their operations. Failure to identify and assess risks to an entity's supply chain can impact the reliable operation of the BES. Failing to identify and assess these risks could allow an entity to install or use a vulnerable product or service from a vendor, allowing threat actors to compromise the entity through its vendor, effectively bypassing security controls established by CIP Reliability Standards.

While purchases that fall under contracts that existed prior to the implementation of CIP-013-1 fall outside the scope of this requirement, there is inherent risk in procuring and deploying BES Cyber Assets into a BES Cyber System that are not being protected at a commensurate level as BES Cyber Assets subject to newer purchasing agreements covered by the entity's plan. Commission staff observed on several occasions unmitigated risk that was present in a BES Cyber System due to assets that had been integrated during the contract term that would have otherwise been minimized if managed within the framework of the supply chain risk management plan parameters required by CIP-013-1, Requirement 1. As stated by the National Institute of Standards and Technology (NIST):[31]

> [E]nterprises should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actional information is learned that indicates that a supplier or a product is a target of a supply chain threat. Supply chains evolve continuously through mergers and acquisitions, joint ventures, and other partnership agreements.

Mitigations

Entities should consider multiple mitigations to enhance supply chain risk management:

1. Review of existing purchasing agreements that pre-date the implementation date of the CIP-013-1 Reliability Standard and integrate applicable BES Cyber Assets into the entity's approach to supply chain risk management, voluntarily applying the provisions of the Reliability Standard.
2. Ensure that the plan(s) implemented pursuant to this requirement address supply chain risks that may arise during the time the contract is in effect. Staff recommends that this approach is applied to all contracts, both those implemented prior to CIP-013-1 and after.
3. Staff has observed several other supply chain risk management best practices applied by industry that may be appropriate to consider when developing a supply chain risk management program:
    a. Identify and prioritize vendors and software based on risk, including those with access to sensitive data, significant functions or shared services, services which could cause operational, compliance, reputational,

31 *See* Boyens, Jon, et. al., *SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST, at 134 (May 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

strategic, and/or credit impacts if breached or disrupted.

b. Identify the makeup and provenance of the vendor's country, and those of the principal members of the organization and board of directors, noting any misalignment with organizational interests and consider contract language provisions to address any identified risks.

c. Ensure hardware, software, and physical security (including cameras) purchases go through a purchase review that includes a cybersecurity review.

d. Implement preventative and detective controls around the purchasing of IT-related equipment to prevent users from circumventing purchase controls.

Additional Guidance

NIST *CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR SYSTEMS AND ORGANIZATIONS*

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

NIST, DHS, CISA *DEFENDING AGAINST SOFTWARE SUPPLY CHAIN ATTACKS*

https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf

NERC *CYBER SECURITY SUPPLY CHAIN RISK MANAGEMENT PLANS – IMPLEMENTATION GUIDANCE FOR RELIABILITY STANDARD CIP-013-2*

https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-013-2_Implementation_Guidance_clean_10072020.pdf

CISA *CYBER SECURITY PROCUREMENT LANGUAGE FOR CONTROL SYSTEMS*

https://www.cisa.gov/sites/default/files/2023-01/Procurement_Language_Rev4_100809_S508C.pdf

DOE *CYBERSECURITY PROCUREMENT LANGUAGE FOR ENERGY DELIVERY SYSTEMS*

https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

2017-2022 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	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-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 Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
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	Requirement R2	Re-evaluate policies, procedures, and controls for Low-impact Cyber Systems and associated Cyber Assets.	**2022**
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 & 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 Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-004-6	Table Requirement 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-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 (PSP).	**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-005-5	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 & CIP-007-6	Requirement R1 & 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 (PSP) 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 (PSPs) periodically to ensure that no unidentified physical access points exist.	**2020**
CIP-006-6	Requirement R1	Limit access to employee's PIN numbers used for accessing PSPs 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 of the parts of the requirement with each manual log, to consistently capture all required information.	**2017**
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 R3.4	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 Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
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-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 Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-007-6 & CIP-010-2	Requirement R2 & 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-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 Requirement 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 Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
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-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 Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
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**

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

FERC.GOV