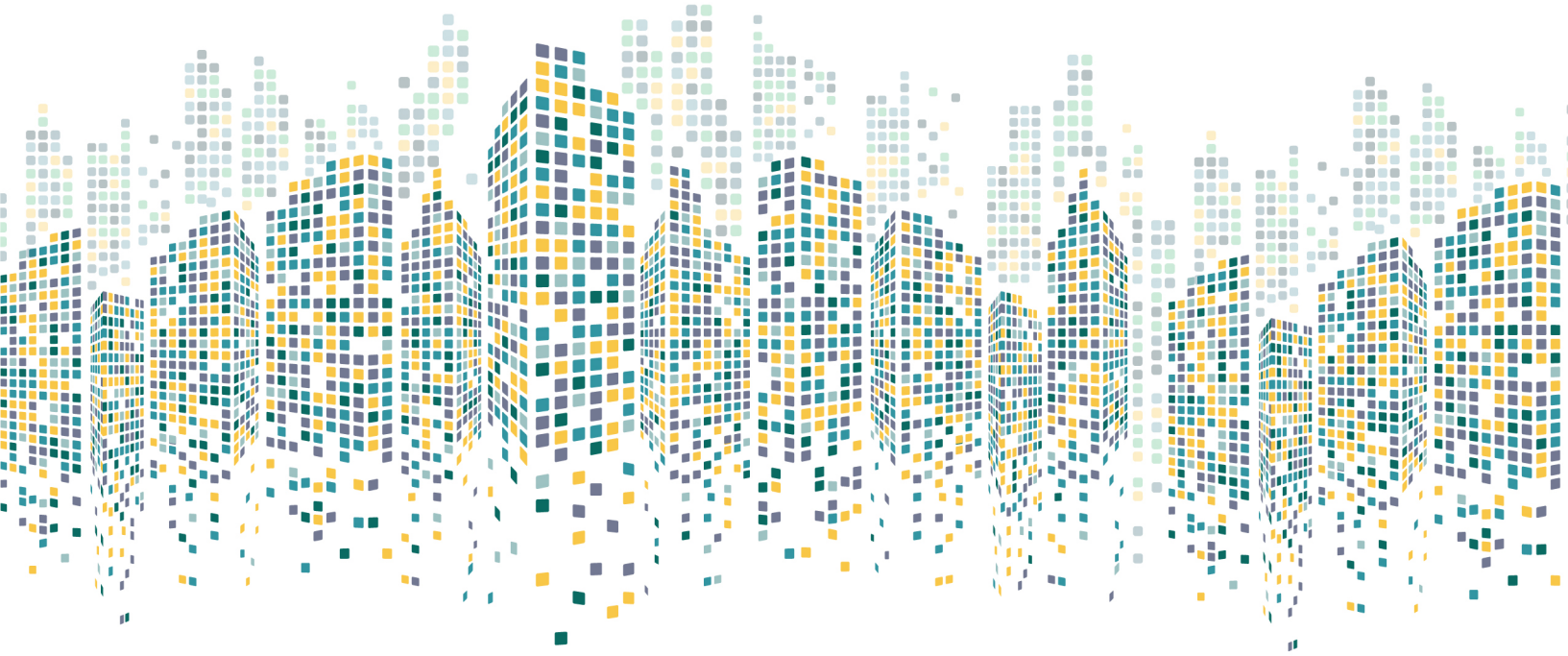
2022 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits



Staff Report
Federal Energy Regulatory Commission
October 2022

2022 Staff Report
Lessons Learned from Commission-Led CIP Reliability Audits

Prepared by Staff of the
Federal Energy Regulatory Commission

Washington, D.C.

October 14, 2022

Contents

Introduction

During Fiscal Year (FY) 2022,[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]

---

[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, FY2022 begins on October 1, 2021 and ends on September 30, 2022.

[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) 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).

[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 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.

This anonymized summary report informs the regulated community and the public of lessons learned from the FY2022 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.

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.[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.

---

[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).

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-003-8 – Security Management Controls
2. CIP-007-6 – Systems Security Management
3. CIP-010-4 – Configuration Change Management and Vulnerability Assessments[10]

[10] The effective date of CIP-010-4 was October 1, 2022. The audits with CIP-010 in scope of review during FY 2022 evaluated compliance with CIP-010-3 (effective July 1, 2020 – September 30, 2022) and CIP-010-2 (effective July 1, 2016 – June 30, 2020).

Audit Scope and Methodology

Audit fieldwork primarily consisted of data requests and reviews, webinars and teleconferences, and virtual on-site visits. Prior to the virtual 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 on-site visits, staff interviewed the entities' subject matter experts and observed demonstrations of operating practices, processes, and procedures used by their staff. 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[11] identified by the registered entity as High, Medium, or Low Impact;[12] 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[13] and Protected Cyber Assets[14] within a BES Cyber

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

[12] 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.

[13] 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.

[14] 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.

System[15] or associated Cyber Assets mainly, but not always, outside the BES Cyber System (i.e., Electronic Access Control or Monitoring Systems (EACMS)[16] and Physical Access Control Systems (PACS)).

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.

[15] The NERC Glossary defines "BES Cyber System" as one or more BES Cyber Assets logically grouped by an entity to perform one or more reliability tasks for a functional entity.

[16] The NERC Glossary defines EACMS as "Cyber Assets that perform electronic access control or electronic access monitoring of the [ESP] or BES Cyber Systems. This includes Intermediate Systems." 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.

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:

1. CIP-003-8, Requirement R2: Re-evaluate policies, procedures, and controls for Low-impact Cyber Systems and associated Cyber Assets.
2. CIP-007-6, Requirement R2.3 & CIP-010-4, 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.
3. CIP-007-6, Requirement R3: Deploy a comprehensive malicious code prevention program for all Cyber Assets within a BES Cyber System.
4. CIP-010-4, Requirement R3: Implement comprehensive vulnerability assessment processes for applicable Cyber Assets.
5. CIP-010-4, Requirement R4: Review and validate controls used to mitigate software vulnerabilities and malicious code on Transient Cyber Assets (TCAs)[17] managed by a third party.

[17] TCAs are generally portable electronic devices used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Lessons Learned Discussion

1. Re-evaluate policies, procedures, and controls for Low Impact Cyber Systems and associated Cyber Assets.

Relates To

CIP-003-8, Requirement R2, Attachment 1

Reliability Standard CIP-003-8 Requirement R2 requires entities with assets containing Low Impact BES Cyber Systems to implement one or more documented cyber security plan(s) that include the sections in Reliability Standard CIP-003-8 Attachment 1. Reliability Standard CIP-003-8 Attachment 1 specifies five security concepts applicable to Low Impact BES Cyber Systems, namely: Cyber Security Awareness, Physical Security Controls, Electronic Access Controls, Cyber Security Incident Response, and TCA and Removable Media Malicious Code Risk Mitigation.

Across all U.S.-based registered entities from 2016 through 2022, there were 21 audit findings identified by Regional Entity, NERC, and Commission-led CIP compliance audits (collectively referred to herein as 'CIP Compliance Audits') related to Reliability Standard CIP-003 Requirement R2.[18] From 2017 to 2018, only one violation per year was reported, with a slight uptick of three violations reported in 2019. Reliability Standard CIP-003 Versions 7 and 8 became effective in 2020 and required more detailed security controls than the previous Version 6, leading to violations of Requirement R2 increasing to five and 11 reported violations in 2020 and 2021, respectively.

Audit staff's analysis of historical findings and experience from recent Commission-led CIP audits demonstrate that security and compliance risks remain. In general, audit staff found entities established policies, procedures, and controls for Low Impact Cyber Systems consistent with CIP-003-8, Requirement R2. However, some entities implemented policies, procedures, and controls to protect Low Impact Cyber Systems and associated Cyber Assets that could benefit from regular re-evaluations to ensure continued effectiveness, particularly for Cyber Security Incident Response and TCAs.

Cyber Security Incident Response

Reliability Standard CIP-003-8, Requirement R2, Attachment 1 section 4 requires entities to have one or more Cyber Security Incident Response Plan(s). Cyber Security Incident Response Plans are intended to guide entities in responding to Reportable Cyber Security Incidents. Regular testing is critical to keep the plans

[18] Audits of U.S.-based registered entities are primarily performed by the Regional Entities, but may also be led by NERC and/or FERC.

current, appropriate, and executable in the event of an incident.[19] It is also important to conduct an initial test to ensure the plan works as intended and the information in the plan is accurate prior to registration. Failure to conduct an initial test could result in errors and delays when the plan is eventually initiated.

During the Commission-led audits conducted during 2022, audit staff learned that the requirement to test a Cyber Security Incident Response plan at least once every 36 calendar months was misinterpreted by certain entities.[20] Specifically, audit staff observed that some entities misinterpreted the requirement to mean Cyber Security Incident Response Plans are not required to be tested until 36 months from registration. The latter is contrary to the NERC Rules of Procedure that requires entity compliance with all applicable Reliability Standards at the time of registration. [21] Thus, the correct understanding of the provision is for an entity to complete a test of its Cyber Security Incident Response Plans prior to registration and to re-test them at least once every 36 calendar months.

With regard to document handling, entities should consider retaining paper (off-line) copies of the Cyber Security Incident Response plan, network diagrams, staff and vendor contacts, and license information. Further, entities should consider regularly exercising Cyber Security Incident Response Plans across organizational business systems to validate the ability to restore compromised systems independently from backup.

For additional guidance on incident response, entities should consider NIST Special Publication 800-61, Computer Security Incident Handling Guide[22] and the SANS Incident Handler's Handbook.[23]

Transient Cyber Assets

Reliability Standard CIP-003-8, Requirement R2, Attachment 1 section 5 requires entities to implement one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to Low Impact BES Cyber Systems

---

[19] CIP-003-8 Supplemental Material, Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response at page 50 of .pdf.

[20] CIP-003-8, Requirement R2, Attachment 1, Section 4, Part 4.5.

[21] *See* NERC Rules and Procedures, Appendix 5A sec. III (requiring all registered entities to be responsible for compliance with all applicable Requirements/sub-Requirements within Reliability Standards).

[22]NIST, *Computer Security Incident Handling Guide*, (Aug. 2012), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[23] SANS, *Incident Handlers Handbook*, (Feb. 2012), https://www.sans.org/white-papers/33901/.

through the use of TCA or Removable Media.[24] Audit staff learned that the requirements for TCAs, as they pertain to Low Impact Cyber Systems, may not be fully understood. Entities must identify all TCAs that it manages as well as those managed by third parties[25] to effectively mitigate the risk, as required by the entity's documented policy and plan associated with those TCAs managed third parties.[26]

TCAs are recognized as a common vector for malicious code transfer into networks and information systems. Failure to implement controls to mitigate the risk of malicious code transfer to BES Cyber Systems presents a serious risk that the BES Cyber Systems may be exposed to, and compromised by, malicious code. The need to implement such controls extends to TCAs not managed by the entity, such as a TCAs used by a contractor to gain access to the entity's BES Cyber System(s).

Entities should consider dedicated TCAs (e.g., laptops) and Removable Media (e.g., USB drives) in the Operational Technology environment. In addition, entities should consider the use of USB port lockdown by use of Group Policy Orchestration toggled on/off based on requirement (Windows environment), and port locks for key critical equipment.

For additional guidance, entities should review NIST Special Publication 800-124 Revision 1;[27] NIST Special Publication 800-82 Revision 3;[28] *Guide to Operational Technology (OT) Security*; and NIST Special Publication 800-53 Revision 5,

[24] Removable Media are generally Universal Serial Bus (USB) drives.

[25] TCAs may be managed by a party other than the Responsible Entity, such as a vendor or a contractor. However, as noted in the Guidelines and Technical Basis for this requirement, this lack of control does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from TCAs it does not manage.

[26] Reliability Standard CIP-003-8 Requirement R2, Attachment 1, Section 5, Part 5.2.

[27] NIST, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*,(June2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

[28] NIST, *Guide to Operational Technology (OT) Security*, (Apr. 2022), (NISTSpecialPublication800-82Revision3), https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft.

Security and Privacy Controls for Information Systems and Organizations; *Guide to Operational Technology (OT) Security*.[29]

2. Address risks posed by end of life/service BES Cyber Assets that have reached the manufacturer-determined end of life/service and are no longer supported by vendors.

Relates to

CIP-007-6, Requirement R2.3

CIP-010-4 Requirement R3.4

Reliability Standard CIP-007-6 Requirement R2.3 requires entities to implement a security patch management program as a proactive way of monitoring and addressing known security vulnerabilities in software to prevent those vulnerabilities being exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

There were 99 audit findings identified across all U.S.-based registered entities from 2016 through 2022 during CIP Compliance Audits related to CIP-007 Requirement R2. These findings trended upward from 2017 through 2020. In addition, audit staff analysis of historical findings and experience from recent Commission-led CIP audits demonstrates that security and compliance risks remain.

During the Commission-led audits conducted during 2022, audit staff found that entities' security patch management and vulnerability assessment programs were compliant with the requirements. However, staff noted multiple instances where the treatment of end-of-life or end-of-service (EOL/EOS) BES Cyber Assets[30] created potential security and compliance risks.[31] Specifically, staff identified that some entities: (1) did not implement a patch management process or create dated mitigation plans for their EOL/EOS BES Cyber Assets without an applicable patch

[29] NIST, *Security and Privacy Controls for Information Systems and Organizations*, (NIST Special Publication 800-82 Revision 5) https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[30] When a particular piece of software or hardware is retired, manufactures no longer supply patches, bug fixes, hot fixes, or security feature upgrades. Threat actors can use these known vulnerabilities to exploit vulnerable EOL/EOS BES Cyber Assets. In a case where a vulnerability has been identified, the vendor may never issue a security patch to address it, deeming the product outdated and obsolete.

[31] EOL/EOS BES Cyber Assets may also affect other CIP Standards such as CIP-010-2 Requirement R3, which pertains to vulnerability assessments. For example, unpatched EOL/EOS BCAs have vulnerabilities that will be identified during the vulnerability assessment process. In these cases, a dated action plan in required to address the vulnerabilities.

source; (2) did not document and inventory EOL/EOS BES Cyber Assets, and thus were unaware of the extent of vulnerable BES Cyber Assets on their system that had reached end of life where the associated vendor no longer supported the hardware or software; and (3) did not have dated action plans to address those EOL/EOS assets as a vulnerability, as required by CIP-010 Requirement R3.4.[32]

Failure to inventory EOL/EOS assets as a vulnerability poses a compliance and security risk. If EOL/EOS are not identified pursuant to an entity's patch management program or its vulnerability assessment program as a vulnerability, security vulnerabilities have an increased risk of being exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable. Additionally, EOL/EOS assets no longer supported by their vendor are susceptible to compatibility issues. For example, if another piece of software, hardware, or service relies on updates, there may be performance and/or reliability issues that may not allow the subject BES Cyber Assets to perform as expected.

Entities should consider removing and/or replacing hardware and software that have reached their EOL/EOS and are no longer supported by the associated vendor as recommended in NIST-800-53.[33] If replacement is not possible or feasible, entities should document, inventory, and communicate what systems and software have reached their EOL/EOS and develop and implement either a dated mitigation plan or a dated action plan for the vulnerabilities that these systems pose to the reliable operation of the BES. The Cybersecurity and Infrastructure Security Agency (CISA) provides a list of "Bad Practices," and first is:

> [u]se of unsupported (i.e., end-of-life) software in service on Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.[34]

3. Deploy a comprehensive malicious code prevention program for all Cyber Assets within a BES Cyber System.

---

[32] Versions 2, 3, and 4 of Reliability Standard CIP-010- Requirement R3.4 require entities to develop and implement a vulnerability assessment process intended to periodically identify and evaluate the risks of security vulnerabilities that may exist, and to develop action plans to remediate or mitigate such vulnerabilities.

[33] NIST, *Security and Privacy Controls for Information Systems and Organizations*, at 290 (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[34] CISA, *Bad Practices*, https://www.cisa.gov/BadPractices.

Required by CIP-007-6, Requirement R3

Reliability Standard CIP-007-6 Requirement R3 provides an approach to implement a malicious code prevention program that protects BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

There were 25 audit findings identified across all U.S.-based registered entities from 2016 through 2022 during CIP Compliance Audits related to CIP-007 Requirement R3. These findings trended upward from 2017 through 2019 and are currently decreasing; however, the security and compliance risk remain. This remaining risk is evident from audit staff's analysis of historical findings and experience from recent Commission-led CIP audits.

During Commission-led CIP audits conducted during 2022, audit staff found entities established processes and controls to deter, detect, and prevent malicious code within the CIP environment. However, in some instances, audit staff observed processes and controls that entities could have implemented more consistently. Specifically, some entities could improve their malicious code prevention programs by: (1) implementing additional controls and practices to detect and mitigate malware and (2) improving methods to deter, detect, or prevent malicious code for non-BES Cyber Assets.

Audit staff found that some entities implemented methods to deter, detect, or prevent malware for BES Cyber Systems that did not have comprehensive and proactive methods to manage, review, and process malware events. For example, proactive investigation of malware detection alerts at a centralized operations center better position entities to deter and prevent malware on BES Cyber Systems as opposed to investigating malware events after-the-fact when the malware may have already compromised an asset(s).

In addition, audit staff found that some entities relied on controls other than anti-virus to deter, detect, or prevent malware for non-windows BES Cyber Assets that did not provide the most effective malware protection, thus exposing security gaps. Such controls included: (1) network controls on non-windows BES Cyber Assets such as allow-listing solutions or Intrusion Detection/Prevention solutions, that were not consistently configured to provide adequate malware protection; (2) asset hardening techniques that were not implemented fully to ensure malware controls were enabled; (3) protections to deter, detect, or prevent malicious code did not exist, and (4) in some cases, compensating controls could not be applied due to EOL/EOS hardware or software.

Lack of proper malware detection or prevention on BES Cyber Assets could lead to misuse and compromise of BES Cyber Systems. If these devices are compromised, lack of detection and prevention capabilities could lead to undetected malware moving across the CIP environment, which could adversely affect reliability of the Bulk-Power System.

Entities should consider additional review of OT firewall logs to identify anomalies and unrecognized traffic attempting to communicate outbound. Additional guidance can be found in NIST Special Publication 800-83.[35] This guide provides recommendations for improving an organization's malware incident prevention measures. The guide also provides extensive recommendations for enhancing an organization's existing incident response capability to be better prepared to handle malware incidents, particularly those incidents that may be widespread.

CISA provides additional publications for consideration, including IR-18-214; R*ecommended Practice: Updating Antivirus in an Industrial Control System*,[36] NIST Special Publication 800-82 Revision 3,[37] *Guide to Operational Technology (OT) Security* SI-3 (Malicious Code Protection) and NIST Special Publication 1058.[38]

4. Implement comprehensive vulnerability assessment processes for applicable Cyber Assets.

Required By

CIP-010-4, Requirement R3

Reliability Standard CIP-010-4 Requirement R3 requires entities to implement a vulnerability assessment program to protect BES Cyber Systems against vulnerabilities, that if exploited, could lead to the compromise of the BES.

There were 41 audit findings identified across all U.S.-based registered entities from 2016 through 2022 during CIP Compliance Audits related to CIP-010-2 and CIP-010-3 Requirement R3. These findings are trending upward consistently since 2016. As a result, the security risks remain.

During Commission-led CIP audits conducted during 2022, audit staff found that while entities generally included multiple vulnerability assessment elements for

[35] NIST, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*,(July2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[36] CISA, Recommended Practice: Updating Antivirus in an Industrial Control System,(Aug.2018), https://www.cisa.gov/uscert/sites/default/files/recommended_practices/Recommended%20Practice%20Updating%20Antivirus%20in%20an%20Industrial%20Control%20System_S508C.pdf.

[37] NIST Special Publication 800-82 Revision 3, *supra* note 28.

[38] NIST, *Using Host-Based Anti-Virus Software on Industrial Control Systems*,(Sep.2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication1058.pdf.

applicable Cyber Assets, in some cases entities did not include key elements in the execution of the vulnerability assessment process. As noted in the Guidelines and Technical Basis for this requirement, entities are strongly encouraged to include at least the following elements in their implementation: network discovery, network port and service identification, vulnerability review and/or scanning, and wireless review and/or scanning.[39] In multiple instances, audit staff noted that one or more of these elements were not performed during the execution of an entity's vulnerability assessments.

Lack of comprehensive vulnerability assessments can lead to the compromise of BES Cyber Assets that can potentially impair BES reliability. Network port and service identification is critical to verify that all enabled ports and services have an appropriate business justification. Vulnerability assessment reviews give a summary of security rule-sets and configurations including controls for default accounts, passwords, and network management settings. Wireless reviews are needed to identify common types of wireless networks and controls relevant to BES Cyber System communications, and failure to do so could leave access points undetected.

Entities should consider updating policy and procedure documentation to incorporate additional security practices in the vulnerability assessment processes for applicable Cyber Assets, to include network port and service identification, wireless review, and vulnerability review. Entities should also address in their vulnerability assessments radio frequencies beyond Wi-Fi (e.g., 6 GHz) that may be used to communicate across significant distances to send telemetry data, as well as issue commands to field assets. In some cases, unencrypted communications would be susceptible to interception, reply, adversary-in-the-middle, and injection attacks,[40] which can be mitigated using encrypted radios. Similarly, substation equipment such as Load Tap Changers[41] allow Bluetooth connectivity, therefore, entities should be aware of default configuration settings on these devices. Entities should consider a full spectrum radio frequency test to identify spectrum in use and

[39] Reliability Standard CIP-010-3, Guidelines and Technical Basis, at 38 of .pdf, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-3.pdf.

[40] Interception attacks allow unauthorized users to access entities' data, applications, or environments, and are primarily an attack against confidentiality. Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail.

[41] Load Tap Changers are used to regulate the output voltage of a transformer.

possible data leakage surrounding the most critical facilities.[42] From a Wi-Fi perspective, the use of Wireless Intrusion Detection/Prevention and rogue access point detection may be helpful to secure and prevent both malicious code and unapproved wireless access points being placed within a protected environment.[43]

Additional guidance can be found in NIST Special Publication 800-115 *Technical Guide to Information Security Testing and Assessment.* Additionally, the National Security Agency (NSA) provides guidance on networking security equipment hardening in the two publications: *Network Infrastructure Security Guide.*

5. Review and validate controls used to mitigate software vulnerabilities and malicious code on TCAs managed by a third party.

Relates To

CIP-010-4, Requirement R4

Requirement R4 of CIP-010-4 is designed to address security-related issues associated with TCAs and Removable Media used by a registered entity or its third-party vendors on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting.[44] TCAs and

[42] In order to detect potential vulnerabilities in radio frequency, penetration testing should be conducted. Penetration testing basically tests the "air" on the exterior and interior of a facility, analyzing the various frequencies being used by radio frequency.

[43] For additional guidance *see* NIST, *Technical Guide to Information Security Testing and Assessment*, (Sep. 2008), https://csrc.nist.gov/publications/detail/sp/800-115/final; https://www.signalsdefense.com/blog/how-you-can-use-rf-penetration-testing/; *see also* NSA, *Network Infrastructure Security Guide*, (June 2022), https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF and NSA, *Cybersecurity Information Sheet*, (Feb. 2022), https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/1/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF (for guidance on networking security equipment hardening).

[44] Reliability Standard CIP-010-4, Requirement R4, provides that "[e]ach Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, one or more documented plan(s) for Transient Cyber Assets and Removable Media" that address the topics set forth in Attachment 1 (titled, "Required Sections for Plans for Transient Cyber Assets and Removable Media") of the Standard. This language remained the same from Version 2 to Version 3 of the Reliability Standard.

Removable Media are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems.[45]

There were 14 audit findings identified across all U.S.-based registered entities from 2016 through 2022 during CIP Compliance Audits related to CIP-010-2 and CIP-010-3 Requirement R4. These findings trended upward from 2017 through 2019, eventually leveling off and sharply decreasing with only two violations between 2020 through 2021. However, experiences from recent Commission-led CIP audits as well as the establishment of other vendor-related related requirements such as CIP-005-6 R2.4 and R2.5 and the requirements found within CIP-013-2, have demonstrated that security and compliance risk remain.

During Commission-led CIP audits conducted during 2022, audit staff found that applicable registered entities reviewed, and validated controls used for the mitigation of software vulnerabilities and malicious code on TCAs managed by a third party (e.g., vendors, contractors) appropriately and in a manner that yielded reasonable assurance that those controls were achieving the requirement objective. However, some entities accepted attestations from third parties without performing due diligence to validate the implementation and performance of the controls being employed met the requirement criteria. Specifically, in some cases, applicable registered entities received attestations from vendors and other third parties with TCAs connected to BES Cyber Assets that identified control objectives that lacked specificity as to how the objectives were to be achieved in practice on the TCA. While assurances were given that the control objectives were being met by the third party's security program, the entities did not routinely attempt to validate the existence and performance of specific measures used to mitigate the risks of software vulnerabilities and malicious code.

Failure to perform a due diligence review of a third party's technical and procedural controls to mitigate the risks of software vulnerabilities and malicious code exposes an entity to an increased risk that these vectors can be used to compromise a BES Cyber System.

Entities should consider validating the specific implementation of controls and associated performance on an asset connecting to its BES Cyber Systems for assurance that the control objectives specified by the requirement are met. Additional methods by which entities may achieve a greater degree of assurance beyond attestations include, but are not limited to: (1) reviewing system owners' applicable security policies and procedures and analyzing their applicability to security requirements; (2) negotiating a "right to audit" the other party; and (3) receiving and reviewing external auditor control assessments and certifications

[45] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-4.pdf.

(e.g., System and Organization Controls 2 reports and International Organization for Standardization 27001 certification).

Looking beyond the methods already discussed above, an emerging concept that may facilitate due diligence validation of security controls for mitigating the threats of malicious code and software vulnerabilities is a Software Bill of Materials" (SBOM). Some system vendors develop SBOMs to enumerate the software packages that make up their products. These inventories can be used to affirmatively determine whether systems are exposed to a known vulnerability based on the versions of underlying software libraries being used. Guidance is still evolving regarding the development and use of SBOMs—specifically in the energy sector through the National Telecommunications and Information Administration[46] and more recently CISA.[47] The opportunity to become involved and engaged with applicable vendors for future capability remains. Additional guidance can be found in NIST Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*,[48] controls CA-2 (Control Assessments), and SA-9 (External System Services) for guidance and best practices. Additionally, NIST hosts a Cybersecurity Supply Chain Risk Management resource page,[49] and the Office of the Director for National Intelligence (ODNI), CISA, and NSA issued a joint paper on *Securing the Software Supply Chain: Recommended Practices for Developers.* [50]

[46] https://www.ntia.gov/SBOM.

[47] https://cisa.gov/sbom.

[48] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[49] https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.

[50] https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF.

2017-2021 Previous Lessons Learned Recommendations[51]

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	**2019**

[51] FERC, *2017 - 2021 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits*,(Oct. 8, 2021), https://www.ferc.gov/sites/default/files/2021-10/2021%20Report%20on%20Commission%20Led%20CIP%20Audits_10.8.21.pdf.

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
		Systems associated with transmission facilities.	
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, 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**

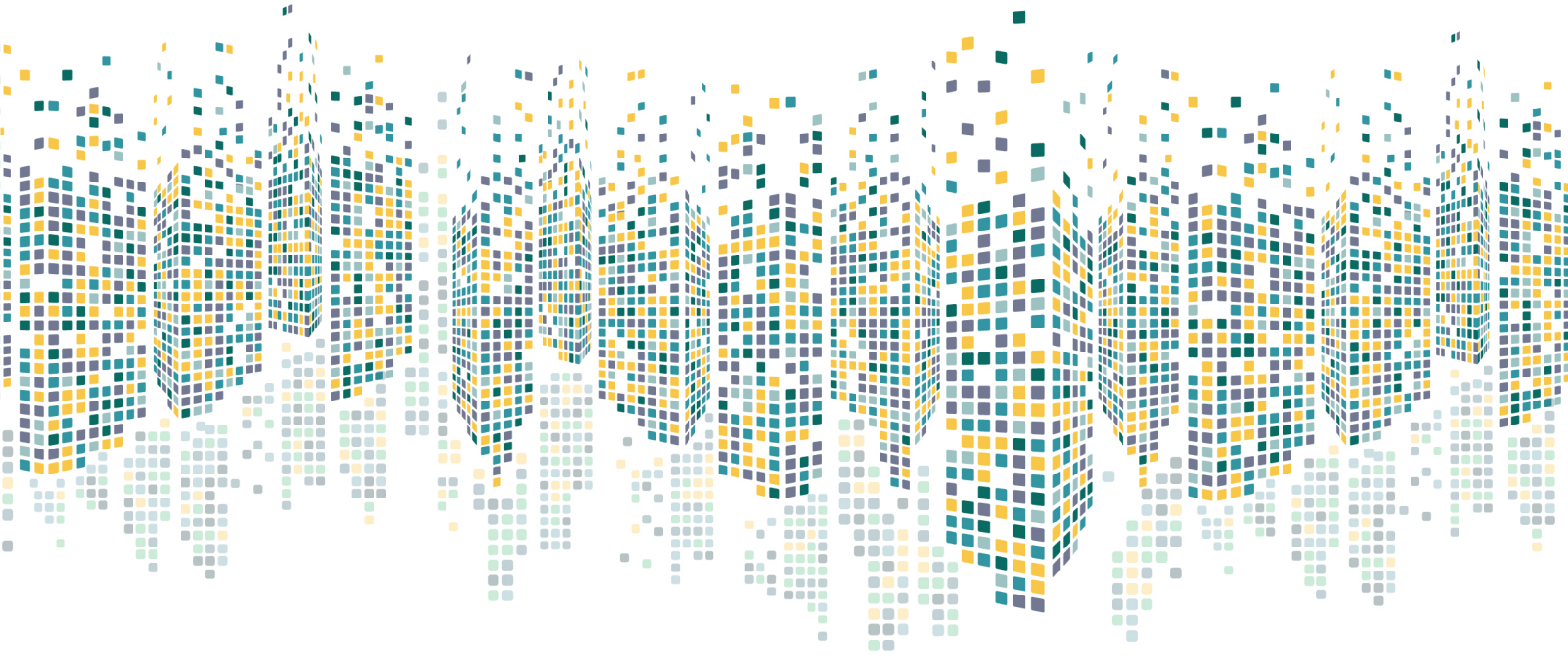
CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-004-6	Requirement R3	Conduct a detailed review of contractor personnel risk assessment processes to ensure sufficiency and to address any gaps.	**2017**
CIP-004-6	Requirement R4	Conduct a detailed review of physical key management 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-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**

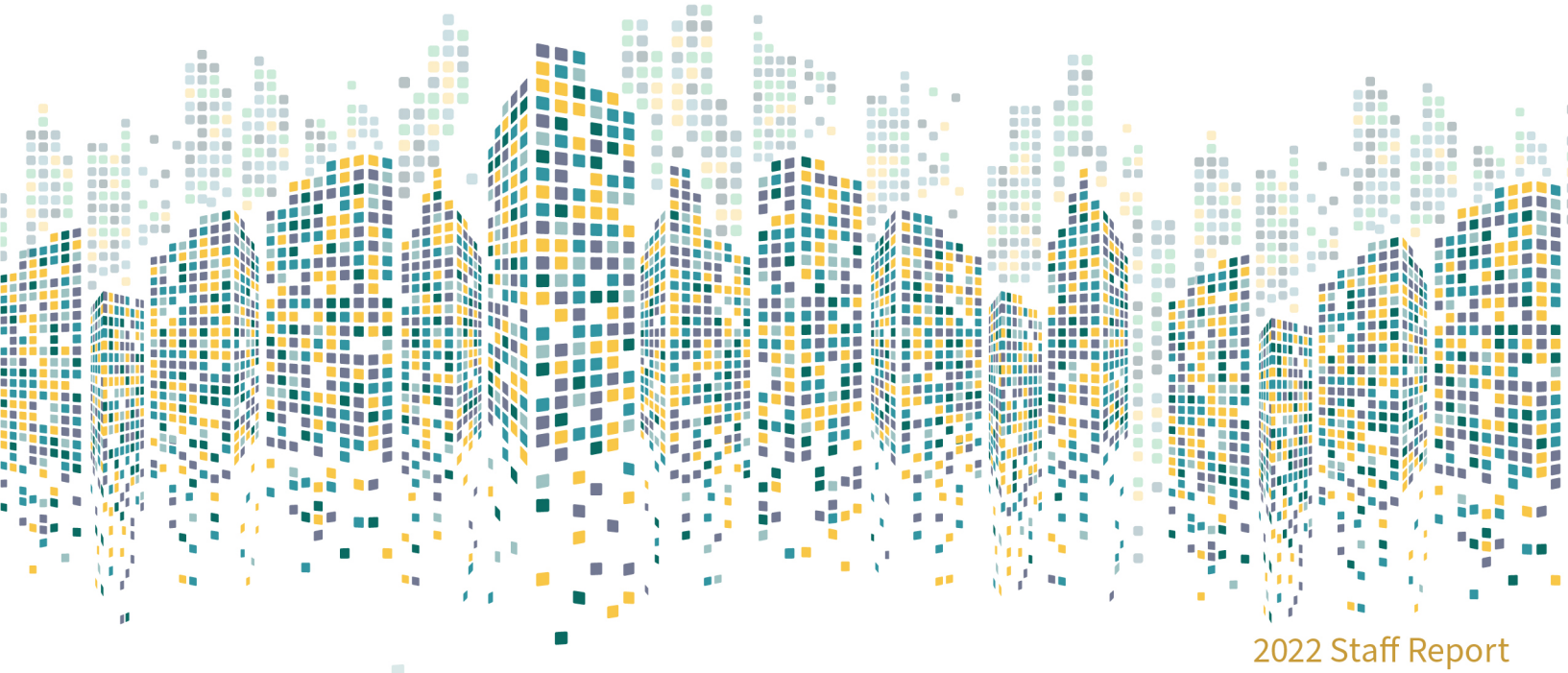
CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-005-5 and CIP-007-6	Requirement R1 and R5	Consider implementing valid Security Certificates within the boundaries of BES Cyber Systems with encryption sufficiently strong to ensure proper authentication of internal connections.	**2018**
CIP-006-6	Requirement R1	Consider having a dedicated visitor log at each Physical Security Perimeter (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	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	**2018**

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
		patching processes and procedures, where appropriate.	
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-010-2	Requirement R3	Consider the remote configuration of applicable Cyber Assets via a TCP/IP-to-RS232 Bridge during vulnerability assessments.	**2018**

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
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-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	**2020**

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
		manage BES Cyber System Information (BCSI).	





2022 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits

Staff Report

Federal Energy Regulatory Commission

October 2022