2021 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits

Staff Report
Federal Energy Regulatory Commission
October 2021

2021 Staff Report
Lessons Learned from Commission-Led CIP Reliability Audits

Prepared by Staff of the
Federal Energy Regulatory Commission

Washington, D.C.

October 8, 2021

Contents

Introduction

During Fiscal Year (FY) 2021,[1] staff of the Federal Energy Regulatory Commission (Commission) completed non-public Critical Infrastructure Protection (CIP) audits (CIP Audits) of several bulk electric system (BES)[2] registered entities.[3] The CIP Audits evaluated registered entities' compliance with the applicable Commission-approved CIP Reliability Standards.[4] Staff from the Regional Entities and the North American Electric Reliability Corporation (NERC) participated in the audits, including the virtual 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 Reliability Standards, there were also potential compliance infractions. Staff also identified practices not required by the CIP Reliability Standards that could improve security, which this report includes as voluntary cyber security recommendations.[5]

This anonymized summary report informs the regulated community and the public of lessons learned from the FY2021 audits. This report provides information and recommendations to NERC, Regional Entities, and registered entities that staff believes

---

[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, FY2021 begins on October 1, 2020 and ends on September 30, 2021.

[2] Section 215 to the Federal Power Act (FPA) gives FERC and NERC (as the Commission-approved Electric Reliability Organization (ERO)) the authority to establish and enforce Reliability Standards on "all users, owners and operators of the bulk-power system." 16 U.S.C. § 824o(b)(1) (2018). NERC's Commission-approved BES definition defines the scope of the Reliability Standards and the entities subject to NERC compliance. *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012).

[3] All Bulk-Power System users, owners and operators are required to register with NERC and, once registered, are commonly referred to as "registered entities."

[4] Compliance with Commission-approved Reliability Standards is mandatory and enforceable for all registered entities pursuant to section 215 of the FPA, 16 U.S.C. § 824o. *See also* 18 CFR. § 39.2(a) (2021).

[5] Although the Office of Energy Infrastructure Security (OEIS) was not involved in these audits, 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 Reliability 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.

are useful 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 security of the BES.

CIP Reliability Standards

Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[6] Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently. The Commission established a process to select and certify an ERO,[7] and subsequently certified NERC.[8] The CIP Reliability 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 Reliability Standards pertaining to cyber security.[9] In addition, the Commission directed NERC to develop certain modifications to the CIP Reliability Standards. Since 2008, the CIP Reliability Standards have undergone multiple revisions to address Commission directives and respond to emerging cyber security issues.

The Commission initiated its CIP Reliability Standards audits of registered entities of the BES in FY2016, and the Commission has conducted CIP audits each year since.

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

1. CIP-002-5.1a – BES Cyber System Categorization
2. CIP-003-8 – Security Management Controls
3. CIP-004-6 – Personnel & Training
4. CIP-007-6 – Systems Security Management
5. CIP-009-6 – Recovery Plans for BES Cyber Systems

---

[6] 16 U.S.C. § 824o.

[7] *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).

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

[9] *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).

6. CIP-010-3 – Configuration Change Management and Vulnerability Assessments
7. CIP-011-2 – Information Protection

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 virtual demonstrations of operating practices, processes, and procedures used by its staff. Additionally, staff virtually interviewed employees and managers responsible for performing tasks within the audit scope and analyzed documentation to verify compliance with requirements; conducted several virtual field inspections and remotely observed the functioning of applicable Cyber Assets[10] identified by the 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

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

[11] The CIP Reliability Standards require that applicable Responsible Entities categorize their BES Cyber Systems and associated Cyber Assets as High, Medium, or Low Impact according to the criteria found in 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, mis operation, 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 Bulk Electric System. 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" as one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

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 entity 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 Reliability Standards requirements, sampling was used to assess compliance.

[15] 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.

[16] The NERC Glossary defines 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 responsible entities improve their compliance with the CIP Reliability Standards and their overall cyber security posture. The lessons learned are presented in order by CIP standard:

1. Enhance policies and procedures to include evaluation of Cyber Asset misuse and degradation during asset categorization.
2. Properly document and implement policies, procedures, and controls for low impact Transient Cyber Assets (TCAs).
3. Implement a defined workflow to enhance processes for the verification of electronic access, unescorted physical access, and access to BES Cyber System Information (BCSI).
4. Base access to BCSI on "need to know."
5. Ensure physical and logical port protection controls for Cyber Assets.
6. Review the system access control program periodically to ensure processes and procedures are implemented as documented.
7. 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.
8. Review configuration change management processes periodically and ensure that they are implemented properly.
9. Enhance configuration change management procedures and controls to document and account for differences between test and production environments.
10. Improve vulnerability assessments to include credential-based scans of Cyber Assets.
11. Properly document and implement policies, procedures, and controls for medium and high impact TCAs.
12. Enhance policies and procedures to include BCSI spillage investigation and response.
13. Enhance policies, procedures, and controls to properly track, document and monitor BCSI storage locations.
14. Enhance internal compliance and controls programs to include control documentation processes and associated procedures pertaining to compliance with the CIP Reliability Standards.

Lessons Learned Discussion

1. Enhance policies and procedures to include evaluation of Cyber Asset misuse and degradation during asset categorization.

Relates To

CIP-002-5.1a Requirement R1

While entities generally identified Cyber Assets effectively, in some cases not all criteria were evaluated consistently. For example, during the classification of BES Cyber Systems, several entities did not consider BES Cyber Asset misuse and degradation, as per the NERC definition for BES Cyber Assets. The entities' categorization criteria were primarily based on unavailability and redundancy of BES Cyber Assets and lacked a commensurate consideration of misuse and degradation. Failing to consider the potential for misuse and degradation could lead to critical assets not being correctly identified as BES Cyber Assets and protected accordingly.

Entities should consider the guidance of the Risk Assessment family of NIST Special Publication (SP) 800-53 Security and Privacy Controls for Information Systems and Organizations.[17] Risk assessments should consider all system components from an account management perspective. System access creates a measurable risk from a misuse and degradation standpoint and will enable identification of applicable BES Cyber Assets. In addition, best practices for an organization would be to conduct a Business Impact Analysis (BIA) and to formalize an Insider Threat Program (InTP). A BIA identifies the impact of a sudden loss of business functions and feeds the creation of a business continuity plan to prioritize recovery of critical business functions in the event of disruption (e.g., cyber-attack). A formalized InTP demonstrates an organization's commitment to conducting due diligence in the protection of its critical assets and provides consistent and repeatable prevention, detection, and responses to insider incidents.

2. Properly document and implement policies, procedures, and controls for low impact Transient Cyber Assets (TCAs).

Required By

CIP-003-8, Requirement R2, Attachment 1, Section 5.2.1

While entities generally had plans and associated internal controls sufficient to mitigate the risk of malicious code to low impact BES Cyber Systems, some controls could be improved. For example, a lack of sufficient controls to ensure procedures were

[17] NIST, *Security and privacy Controls for Information Systems and Organizations*, Special Publication 800-53 Revision 5 (NIST SP 800-53) (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (a publication developed by NIST as part of its statutory responsibilities establishing information security standards and guidelines, including minimum requirements for federal information systems).

followed resulted in an incomplete review of antivirus level updates of a third-party TCA prior to the third-party connecting that TCA to the entities' low impact Cyber Asset. Failure to ensure that third party TCAs undergo antivirus review prior to connection to Cyber Assets presents the risk that the Cyber Assets may be exposed to and compromised by malicious code.

Entities should consider the guidance of the System and Information Integrity (SI) family of NIST SP 800-53. The SI family provides the baseline criteria for deploying sustainable security control configurations for the detection and mitigation of malicious code. The series of controls, as mapped by the SI family, would address third-party asset review as described above.

3. Implement a defined workflow to enhance processes for the verification of electronic access, unescorted physical access, and access to BES Cyber System Information (BCSI).

Required by CIP-004-6, Requirement R4

Some entities implemented access control workflow that did not have a consistent process to verify the implementation of its access control programs, including: (1) at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records; and/or (2) at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are accurate. For example, some entities' access verification procedures did not specify an order for the authorization and approval by required individuals. Entities should consider enhancing their quarterly and annual access review authorization processes, controls, and training by implementing a workflow where the direct line manager's review occurs after the system owner's review to ensure there are no conflicting authorizations. By not having established workflows, entities may allow a user to continue accessing BES Cyber System Information (BCSI) information without having the need for such access.

Entities should consider the guidance of the Access Control (AC) family of NIST SP 800-53. The AC family addresses privileged account management in detail to include reoccurring account verification, the principle of least privilege, and policies dictating the timely modification of account access to mitigate insider threat. The series of controls also addresses the policy aspects of account management to ensure optimized workflows.

4. Base access to BCSI on "need to know."

Required By CIP-004-6, Requirement R4.1.3

In general, entities appropriately authorized electronic access, unescorted physical access, and access to designated electronic storage locations for BCSI. However, some entities did not consistently apply their documented process to properly authorize access to BCSI based on need, as determined by the entity. For example, entities did not follow access control procedures which required any access, permanent or temporary, to be authorized and justified in an access request before the access was provisioned. Failure to restrict unauthorized electronic access, unescorted physical

access, and BCSI access by way of specific information protection requirements in support of protecting BES Cyber Systems against compromise could lead to mis-operation or instability in the Bulk Electric System.

Entities should consider the guidance of the AC family of NIST SP 800-53. The AC family contains an extensive section guiding entities through the proper documentation of account management policy to ensure consistent and repeatable application. Entities would also benefit from the AC family's coverage of Role-Based Access Control under its Access Enforcement section.

5. Ensure physical and logical port protection controls for Cyber Assets.

Relates To
CIP-007-6, Requirement R1

In general, entities established physical and logical port protection procedures and controls for Cyber Assets. However, not all entities consistently implemented adequate physical and logical port protection controls for Cyber Assets. Specifically, some entities could enhance their ports and services policies and procedures by including: (1) a formal process for capturing sufficient details and improved justification documentation for logical network accessible ports and (2) internal controls to ensure all justifications are completed for logical network accessible ports.

Some entities documented processes for identifying, documenting, and reviewing logical network accessible ports, but did not provide details as to what to include in the justifications for each open logical port on each Cyber Asset. For example, logical network accessible ports documentation for a Cyber Asset listed the justification as "system monitoring," which is the function and not a complete justification for the open port. Incomplete documentation for the justification of ports and services usage within the CIP environment makes verification difficult and could lead to unnecessary ports and services remaining open.

Entities should consider the guidance of the Configuration Management (CM) family of NIST SP 800-53. The CM family covers the concept of "Least Functionality" and addresses system mapping, risk analysis, optimized configuration deployment, and proper documentation.

6. Review the system access control program periodically to ensure processes and procedures are implemented as documented.

Required By
CIP-007-6, Requirement R5

In general, entities properly maintained adequate documented processes and procedures for system access control; however, some entities continue to have challenges implementing certain elements of the system access control program as mentioned in a previous lesson learned report.[18]

[18] *See* 2017 Staff Report Lessons Learned from Commission-Led CIP Version 5 Reliability Audits (Oct. 6, 2017), https://www.ferc.gov/sites/default/files/2020-05/10-06-17-CIP-audits-report_0.pdf.

For example, some entities did not have a documented process to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, as required by CIP-007-6, Requirement R5, Part 5.7. The implementation of controls is an important step in a risk management program. In addition, formally documenting policies, processes, and procedures is essential to the success of the overall risk management program.

Documented processes are essential for many reasons, including consistency, efficiency, process improvement, and training. Not having a documented process for limiting the number of unsuccessful authentication attempts and/or generating alerts after a threshold of unsuccessful authentication attempts could undermine the effectiveness of the entity's efforts and lead to inconsistency and human error, potentially exposing BES Cyber Assets to password attacks. Entities should consider National Security Agency (NSA) best practice guidance to prevent and detect brute force password guessing:

> Use multi-factor authentication with strong factors and require regular re-authentication, enable time-out, and lock-out features whenever password authentication is needed. Time-out features should increase in duration with additional failed login attempts. Lock-out features should temporarily disable accounts after many consecutive failed attempts. This can force slower brute force attempts, making them infeasible. Some services can check passwords against common password dictionaries when users change passwords, denying many poor password choices before they are set. This makes brute-force password guessing far more difficult and use automated tools to audit access logs for security concerns and identify anomalous access requests.[19]

7. 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.

Required By

CIP-009-2, Requirement R2

While entities generally maintained documented processes for the backup and storage of information required to recover BES Cyber System functionality, some entities failed to include a sample of data from offsite backup storage locations in the representative sample of data used to test the restoration of BES Cyber Systems. When developing a sampling methodology to determine a representative sample, entities should consider the uniqueness of historical backups' data being stored at offsite data storage nodes.

A formalized recovery plan should reflect, at minimum, critical mission system dependencies, recovery time objectives, and build documents for identified servers. A recovery plan, at a minimum, includes verified off-site backups, operating system build software and required licenses. Also consider the use of fully off-line backups and cloud-based infrastructure, and immutable storage to combat attacks targeting storage solutions (i.e., ransomware). Entities should consider the guidance of the Contingency Planning

[19] https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/0/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.

control family of NIST SP 800-53. For example, entities should consider systematic preservation of system documentation.

8. Review configuration change management processes periodically and ensure that they are implemented properly.

Relates To
CIP-010-3, Requirement R1

Entities generally implemented appropriate procedures to document and monitor baseline configurations of their Cyber Assets; however, some entities could improve the policies, procedures, and controls for tracking, documenting, and monitoring baseline configurations for Cyber Assets. For example, staff noted that in some cases entities did not accurately record all parts of baseline configurations and had limited information on ports. While CIP-010-3 R1 requires information on five areas of baseline configurations for Cyber Assets, staff noted only two or three parts would be provided by entities when submitting compliance documentation. Errors in documenting baselines may lead to an inaccurate assessment of an entity's security posture. If an entity is not aware of the hardware and software it has installed, it may also be unaware of the vulnerabilities of those Cyber Assets, which may lead to inadequate protection of the Cyber Assets.

9. Enhance configuration change management procedures and controls to document and account for differences between test and production environments.

Relates To
CIP-010-3, Requirement R1.5

Some entities did not have consistent policies and procedures for documenting test and production environments. Staff observed potential risks and areas for improvement of documented process to better reflect: (1) differences between the test environment and the production environment; and (2) measures used to account for any differences in the environments. If a test/model environment is used, it is important to fully document differences between it and the production environment, as well as the measures used to account for the differences. Doing so should enable the entity to better anticipate and avoid any negative consequences of implementing the configuration change in the production environment.

Entities should consider the guidance of the CM family of NIST SP 800-53. The CM family maps all related security controls covering configuration change implementation within the operational environment. It will assist entities in addressing the transition of configuration changes from a test environment to a full production network as described above. In addition, best practices relative to change controls include, among others, the establishment of a formal change control board and ensuring that the test environment accurately emulates the development and production environments requiring different credentials between environments.

10. Improve vulnerability assessments to include credential-based scans of BES Cyber Assets.

Relates To

CIP-010-3, Requirement R3

When performing vulnerability assessments, some entities chose to perform non-credential-based vulnerability scans to scan Cyber Assets instead of performing credential-based scans. Non-credentialed scans do not require credentials and do not provide trusted access to the systems they are scanning. Therefore, non-credentialed scans may not accurately identify all vulnerabilities and weaknesses within the system. Conversely, credential-based scans use a credentialed account to log into a system and identify a definitive list of vulnerabilities and weaknesses within the system. In addition, vulnerability assessments should scan for out of band ports, also referred to as a management network, (e.g., Integrated Lights Out Management (iLOM), Dell Remote Access Controller (DRAC)) and firmware supporting out of band management solutions to ensure versions are up to date.

The vulnerability assessment process acts as one of the components in an overall security program and helps to improve the security posture of BES Cyber Systems. Failure to thoroughly identify and assess the vulnerabilities and weaknesses of Cyber Assets can lead to possible compromise of Cyber Assets and negative reliability impacts of the entity's Cyber Systems.

Entities should consider NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. The purpose of this document is to provide guidelines for organizations on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies.

11. Properly document and implement policies, procedures, and controls for medium and high impact TCAs.

Required By

CIP-010-3, Requirement R4

Entities generally implemented sufficient procedures and controls to properly handle and protect TCAs and removable media; however, some entities did not have adequate security patch management policies, procedures, and controls to identify, track, and mitigate security vulnerabilities on TCAs. For example, some entities ran multiple versions of the same operating system (OS) on its TCAs that were several security versions behind current versions. While CIP-010-3 R4 requires security patch updates be applied to all applicable Cyber Assets, it does not require upgrades. By not choosing to upgrade the OS, some entities did not identify, track, and mitigate security vulnerabilities that existed on OSs that had reached end of life (EOL)/end of service (EOS).

EOL/EOS versions of OS are vulnerable to exploitation because they have not been patched or upgraded with security updates to protect against current exploitation. Unpatched systems with known vulnerabilities are a sought-after attack vector by attackers, and malicious actors quickly develop exploits for newly discovered vulnerabilities. The lack of OS upgrades and patching for TCAs to address such vulnerabilities could lead to exploitation of security vulnerabilities in a malicious manner in order to gain control of, or render a TCA, Cyber Asset, or BES Cyber System inoperable.

12. Enhance policies and procedures to include BCSI spillage investigation and response.

Relates To
CIP-011-2, Requirement R1.2

Entities should implement procedures for the investigation of BCSI spillage incidents that include the purging of spilled data from applicable data backups stored within backup data storage nodes.

Some entities' processes for the investigation of BCSI spillage incidents were "ad hoc" and lacked formal procedures for handling such incidents. For example, in some cases BCSI spillage incident investigations did not include review of backup data instances. Entities should consider enhancing policies, procedures, and controls to ensure BCSI spillage incidents are handled accordingly.

Lack of policy and procedures for handling BCSI spillages can lead to BCSI accidentally made available to unauthorized parties. Best practices relative to investigating the spillage of sensitive data include, among others, a formalized incident response process that includes containment, forensics, and the preservation of evidence as well as a playbook specifically developed to address data spills. Additionally, formalized social media and personal electronic device policies that address photos and posting of information considered sensitive (e.g., marker boards, operations centers, phone lists, computer screens, access badges, security monitors, maps, critical systems) are recommended. The deployment of a properly configured and maintained automated Data Loss Prevention system is also recommended.

Entities should consider NIST SP-209, Security Guidelines for Storage Infrastructure. The purpose of this document is to provide comprehensive set of security recommendations for the current landscape of the storage infrastructure.

13. Enhance policies, procedures, and controls to properly track, document and monitor BCSI storage locations.

Relates To
CIP-011-2, Requirement R1.1.2

While entities generally implemented policies, procedures, and controls for BCSI and associated BES Cyber Systems, the process and implementation could be improved. Entities should specifically consider the following:

Physical Requirements:

1) Revise procedures and controls to comprehensively address monitoring and tracking of physical BCSI.
2) Identify physical BCSI storage locations
3) Document Physical BCSI storage locations.

Electronic Requirements:

1) Re-evaluate methods for identifying BCSI and associated BES Cyber Systems.
2) Review all data sources and ensure all BCSI is properly identified.

3) Re-evaluate BCSI access and protection measures.

Failing to properly identify, track, document and monitor information associated with a BES Cyber System as BCSI presents a risk of the information being compromised or unauthorized access and exploitation. Best practices relative to tracking and properly handling physical information include, among others, establishing policies and procedures for the proper categorization and marking of sensitive data as well as a formal data destruction policy that includes provisions for properly disposing of sensitive physical information (e.g., hard drives and volatile memory). Entities may enhance security of electronic data through the use of meta-data and header/footer tagging to communicate the sensitivity level of the document to users and electronic information-handling mechanisms.

14. Enhance internal compliance and controls programs to include control documentation processes and associated procedures pertaining to compliance with the CIP Reliability Standards.

Relates To
All CIP Requirements

While entities generally had internal compliance and controls programs in place pertaining to many aspects of their operations, there were instances of insufficient incorporation and application of these programs to operating processes intended to help mitigate risk of noncompliance with the CIP Reliability Standards. NERC has advised that effective internal controls support the reliability and security of the BPS by identifying, assessing, and correcting issues; and their performance can demonstrate reasonable assurance of compliance with CIP Reliability Standards.[20] Moreover, not having well-defined, documented, and periodically verified internal control processes could result in unmanaged and unmitigated risks to the BPS.

Entities should consider the guidance of the SI family of NIST SP 800-53 and other relevant publications. Best practices entities may implement to enhance their internal control programs and processes include: (1) ensuring that controls are appropriately mapped to applicable Reliability Standards and Requirements; (2) including detailed control descriptions in compliance and controls programs documentation (3) linking implemented controls to documentation on objectives and related risks; and (4) retaining documentation supporting the operation of internal controls such that the design and operating effectiveness of internal controls can be demonstrated and evaluated. In addition, entities should consider an independent review and evaluation of their compliance and controls programs, specifically in areas where segregation of duties could be a relevant component of an internal control program but cannot be achieved due to resource constraints.

[20] NERC, *ERO Enterprise Guide for Internal Controls*, Version 2, Sept. 2017, available at https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Guide_for_Internal_Controls_Final12212016.pdf.

Previous Lessons Learned Recommendations

2020 Lessons Learned[21]

1. Ensure that all BES Cyber Assets are properly identified.
2. Ensure that all substation BES Cyber Systems are properly categorized as high, medium, or low impact.
3. Ensure that access to BES Cyber System Information is properly authorized and revoked.
4. Consider having a dedicated visitor log at each Physical Security Perimeter (PSP) access point.
5. Consider locking BES Cyber Systems' server racks where possible.
6. Inspect all PSPs periodically to ensure that no unidentified physical access points exist.
7. Review security patch management processes periodically and ensure that they are implemented properly.
8. Consider consolidating and centralizing password change procedures and documentation.
9. Ensure that backup and recovery procedures are updated in a timely manner.
10. Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.
11. Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.
12. 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 BCSI.

2019 Lessons Learned[22]

1. Consider all generation assets, regardless of ownership, when categorizing BES Cyber Systems associated with transmission facilities.
2. Ensure that all employees and third-party contractors complete the required training and that the training records are properly maintained.
3. Verify employees' recurring authorizations for using removable media.
4. Review all firewalls to ensure there are no obsolete or overly permissive firewall access control rules in use.
5. Limit access to employees' PIN numbers used for accessing PSPs using a least-privilege approach.

---

[21] *See* 2020 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits (Oct. 9, 2019), https://www.ferc.gov/media/2020-staff-report-lessons-learned-commission-led-cip-reliability-audits.

[22] *See* 2019 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits (Oct. 4, 2019), https://www.ferc.gov/sites/default/files/2020-05/10-04-19_2.pdf.

6. Ensure that all ephemeral port ranges are within the Internet Assigned Numbers Authority recommended ranges.
7. Clearly mark TCAs and Removable Media.

2018 Lessons Learned[23]

1. 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.
2. Consider implementing valid Security Certificates within the boundaries of BES Cyber Systems with encryption sufficiently strong to ensure proper authentication of internal connections.
3. 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.
4. Consider Internet Control Message Protocol as a logical access port for all the BES Cyber Assets.
5. Enhance documented processes and procedures for incident response to consider the NIST SP 800-61, "Computer Security Incident Handling Guide."
6. Consider the remote configuration of applicable Cyber Assets via a TCP/IP-to-RS232 Bridge during vulnerability assessments.
7. Consider the use of secure administrative hosts to perform administrative tasks when accessing either EACMS or PACS.
8. Consider replacing or upgrading "End-of-Life" system components of an applicable Cyber Asset.
9. Consider incorporating file verification methods, such as hashing, during manual patching processes and procedures, where appropriate.
10. Consider using automated mechanisms that enforce asset inventory updates during configuration management.

2017 Lessons Learned[24]

1. 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.

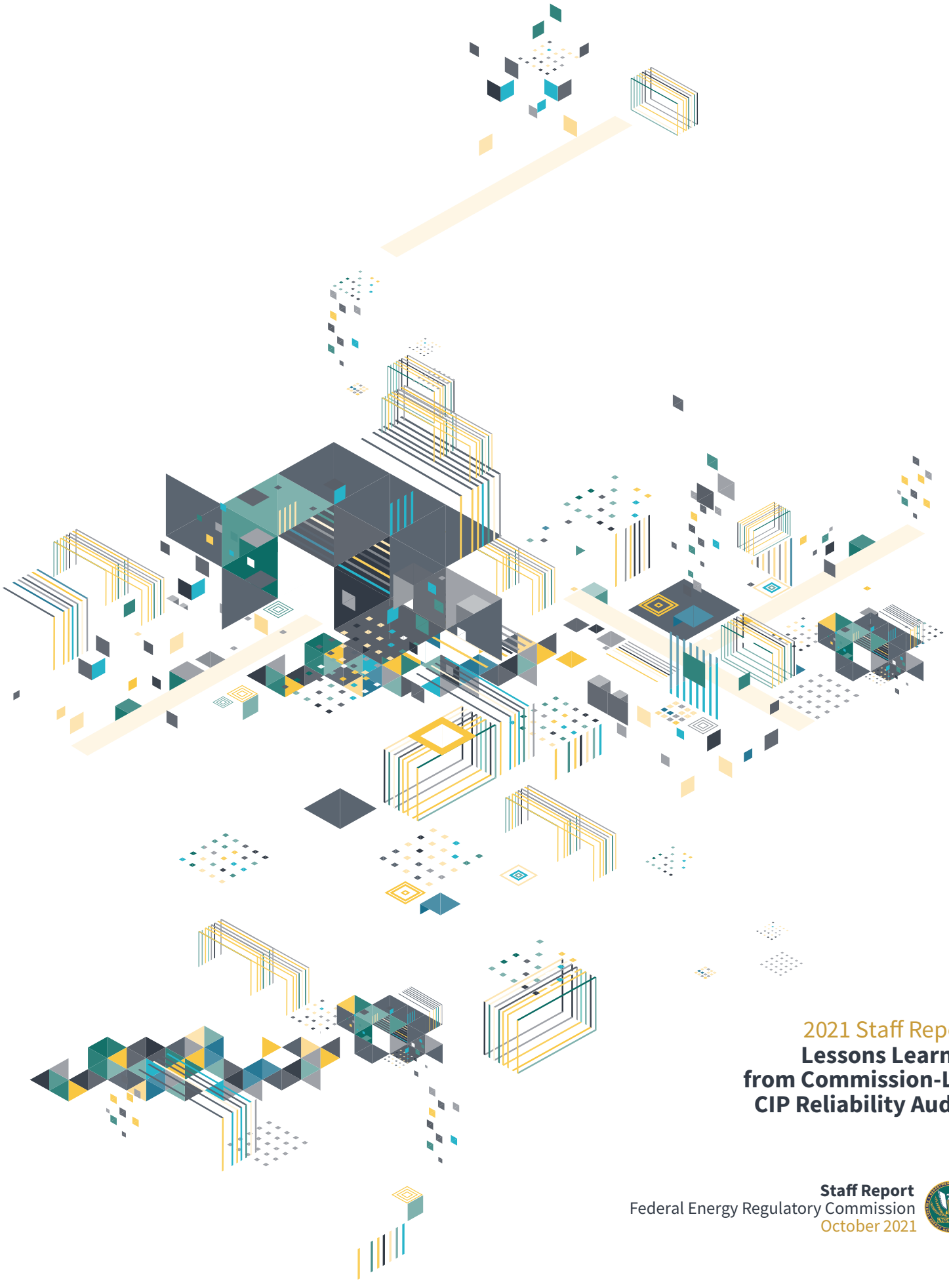
---

[23] *See* 2018 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits (Feb. 6, 2019), https://www.ferc.gov/sites/default/files/2020-05/2018-report-audits_0.pdf.

[24] *See* 2017 Staff Report Lessons Learned from Commission-Led CIP Version 5 Reliability Audits (Oct. 6, 2017), https://www.ferc.gov/sites/default/files/2020-05/10-06-17-CIP-audits-report_0.pdf.

2. 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.
3. Consider all owned generation assets, regardless of BES-classification, when evaluating impact ratings to ensure proper classification of BES Cyber Systems.
4. Identify and categorize cyber systems used for supporting generation, in addition to the cyber systems used to directly control generation.
5. 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.
6. Conduct a detailed review of contractor personnel risk assessment processes to ensure sufficiency and to address any gaps.
7. 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 PSP.
8. Enhance procedures, testing, and controls around manual transfer of access rights between personnel accessing tracking systems, PACS, and EACMS or, alternatively, consider the use of automated access rights provisioning.
9. Ensure that access permissions within personnel access tracking systems are clearly mapped to the associated access rights within PACS and EACMS.
10. Ensure that policies and testing procedures for all electronic communications protocols are afforded the same rigor.
11. Perform regular physical inspections of BES Cyber Systems to ensure no unidentified electronic access points exist.
12. Review all firewall rules and ensure access control lists follow the principle of "least privilege."
13. For each remote Cyber Asset conducting 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.
14. 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.
15. 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.
16. 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.
17. Implement procedures and controls to monitor or limit the number of simultaneously successful logins to multiple different systems.
18. Implement procedures to detect and investigate unauthorized changes to baseline configurations.
19. Ensure that all commercially available enterprise software tools are included in BSCI storage evaluation procedures.

20. Enhance documented processes and procedures for identifying BCSI to consider the NERC Critical Infrastructure Protection Committee guidance document, "Security Guideline for the Electricity Sector: Protecting Sensitive Information."
21. Document all procedures for the proper handling of BCSI.



2021 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits

Staff Report
Federal Energy Regulatory Commission
October 2021