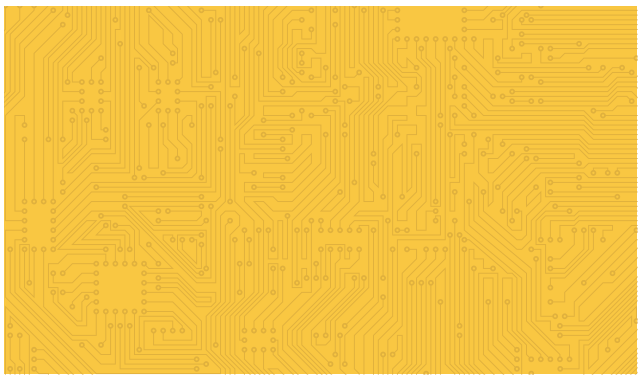
2019 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits



Staff Report
Federal Energy Regulatory Commission
October 2019

Lessons Learned from Commission-Led CIP Reliability Audits

Prepared by Staff of the

Federal Energy Regulatory Commission

Washington, D.C.

October 4, 2019

FEDERAL ENERGY REGULATORY COMMISSION

The matters presented in this staff report do not necessarily represent the views of the Federal Energy Regulatory Commission, its Chairman, or individual Commissioners, and are not binding on the Commission.

Table of Contents

I. Introduction

During Fiscal Year (FY) 2019,[1] the staff of the Division of Reliability Standards and Security in the Office of Electric Reliability (OER), with assistance of staff of the Division of Audits and Accounting in the Office of Enforcement, of the Federal Energy Regulatory Commission (Commission) has completed non-public Critical Infrastructure Protection (CIP) audits (CIP Audits) of several "registered entities"[2] of the bulk electric system (BES).[3] The CIP Audits evaluated registered entities' compliance with the applicable Commission-approved CIP Reliability Standards.[4] Staff from Regional Entities and the North American Electric Reliability Corporation (NERC) participated in the audits, including the on-site portion.

During the CIP Audits, staff found that most of the cyber security protection processes and procedures adopted by the registered entities met the mandatory requirements of the CIP Reliability Standards. However, there were also potential compliance infractions found. Additionally, staff observed practices that could improve security but are not necessarily required by the CIP Reliability Standards. Therefore, this report includes recommendations regarding cybersecurity practices that are voluntary.[5] Similar observations derived from audits carried out in FY16 and FY17 were shared with the industry in the 2017 Lessons

[1] The fiscal year is the accounting period for the federal government which begins on October 1 and ends on September 30. The fiscal year is designated by the calendar year in which it ends; for example, fiscal year 2019 begins on October 1, 2018 and ends on September 30, 2019.

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

[3] BES is defined in the "Glossary of Terms Used in NERC Reliability Standards" (NERC Glossary), http://www.nerc.com/files/glossary_of_terms.pdf.

[4] Compliance with Commission-approved Reliability Standards is mandatory and subject to enforcement pursuant to section 215 of the Federal Power Act, 16 U.S.C. 824o, and Part 40 of the Commission's regulations, 18 C.F.R. Part 40 (2019).

[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.

Learned Report,[6] and observations derived from audits carried out in FY18 were shared with the industry in the 2018 Lessons Learned Report.[7]

The CIP Audits are non-public. This anonymized summary report informs the regulated community and the public of additional lessons learned from the FY19 audits. This report provides information and recommendations to NERC, regional entities, and registered entities that staff believes are useful in their assessments of risk and compliance, and to overall cyber security. Moreover, this information may be generally beneficial to the utility-based cyber security community to improve the security of the BES.

[6] *See* 2017 Staff Report Lessons Learned from Commission-Led CIP Version 5 Reliability Audits (Oct. 6, 2017), https://www.ferc.gov/legal/staff-reports/2017/10-06-17-CIP-audits-report.pdf.

[7] *See* 2018 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits (Feb. 6, 2018), https://www.ferc.gov/legal/staff-reports/2019/2018-report-audits.pdf.

II. CIP Reliability Standards

Section 215 of the Federal Power Act (FPA) requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[8] 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,[9] and subsequently certified NERC.[10] The CIP Reliability Standards are designed to mitigate the cybersecurity and physical security risks to BES facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cybersecurity 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 cybersecurity.[11] 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 cybersecurity issues.

The Commission initiated its cybersecurity CIP Reliability Standards audits of registered entities of the BES in FY16. The cybersecurity audits focused on evaluating compliance with CIP Reliability Standards version 5 (CIP v5) for periods after July 1, 2016.[12] The Commission also evaluated compliance with CIP Reliability Standards version 3 (CIP v3),

---

[8] 16 U.S.C. 824o (2012).

[9] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g,* Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[10] *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).

[11] *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).

[12] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037 (2016), *reh'g denied*, 156 FERC ¶ 61,052; Reliability Standards: CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2; *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, 146 FERC ¶ 61,188 (2014); Reliability Standards: CIP-002-5.1a, CIP-005-5, and CIP-008-5.

for the period of each audited entity's last CIP compliance audit through June 30, 2016 (the effective end date of CIP v3).[13]

The CIP Reliability Standards can 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-003-6 – Security Management Controls
3. CIP-004-6 – Personnel & Training
4. CIP-005-5 – Electronic Security Perimeter(s)
5. CIP-006-6 – Physical Security of BES Cyber Systems
6. CIP-007-6 – Systems Security Management
7. CIP-008-5 – Incident Reporting and Response Planning
8. CIP-009-5 – Recovery Plans for BES Cyber Systems
9. CIP-010-2 – Configuration Change Management and Vulnerability Assessments
10. CIP-011-2 – Information Protection

[13] *Revised Reliability Standards for Critical Infrastructure Protection*, 128 FERC ¶ 61,291, *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009), *order on compliance*, 130 FERC ¶ 61,271 (2010); Reliability Standards: CIP-002-3, CIP-003-3, CIP-004-3, CIP-005-3, CIP-006-3, CIP-007-3, CIP-008-3, and CIP-009-3.

III. Audit Scope and Methodology

Audit fieldwork primarily consisted of data requests and reviews, webinars and teleconferences, and a site visit to each entity's facilities. Prior to a site visit, staff issued data requests to gather information pertaining to an entity's 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 a site visit, staff interviewed an entity's subject matter experts; observed operating practices, processes, and procedures used by its staff in real-time; and examined its functions, operations, practices, and regulatory and corporate compliance culture. 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 and observed the functioning of applicable Cyber Assets[14] identified by an entity as High, Medium, or Low Impact;[15] 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[16] and Protected Cyber Assets[17] within a BES Cyber System[18] or associated Cyber Assets outside the BES Cyber System (*i.e.*, Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)).

The data, information, and evidence provided by an entity were evaluated for sufficiency, appropriateness, and validity. Documentation submitted in the form of policies, procedures, e-mails, logs, studies, data, etc., were validated, substantiated, and crosschecked for accuracy

---

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

[15] 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.

[16] 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 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.

[17] The NERC Glossary defines "Protected Cyber Asset" as a Cyber Asset connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. 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.

[18] 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.

as appropriate. For certain CIP Reliability Standards Requirements, sampling was used to test compliance.

IV. Overview of Lessons Learned

The lessons observed and discussed in this report are derived from the FY19 CIP Audits with assistance from OEIS staff. These lessons learned are intended to help responsible entities to improve their compliance with the CIP Reliability Standards and their overall cyber security posture.

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 employee's PIN numbers used for accessing PSPs using a least-privilege approach.
6. Ensure that all ephemeral port ranges are within the Internet Assigned Numbers Authority (IANA) recommended ranges.
7. Clearly mark Transient Cyber Assets and Removable Media.

V. Lessons Learned Discussion

1. Consider all generation assets, regardless of ownership, when categorizing BES Cyber Systems associated with transmission facilities.

Relates To

CIP-002-5.1a R1 Attachment 1 Criterion 2.8

While entities generally categorized BES Cyber Systems effectively, in some cases entities did not consider all generation facilities as required. In particular, pursuant to CIP-002-5.1a, Attachment 1, Criterion 2.8, entities should consider "facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3" when evaluating the potential impact of lost transmission facilities on the availability of generation facilities. Staff observed, however, that some entities only considered the loss of its own generation facilities when evaluating the potential impact of its transmission facilities being rendered unavailable.

2. Ensure that all employees and third-party contractors complete the required training and that the training records are properly maintained.

Relates To

CIP-004-6, Requirement R2

Entities generally maintained complete training records for employees who have been granted authorized electronic access and/or authorized unescorted physical access to applicable Cyber Assets. However, some entities did not maintain complete training records for their third-party contractors.

3. Verify employee's recurring authorization for using removable media.

Relates To

CIP-004-6, Requirement R4

Reliability Standard CIP-004-6, Requirement 4, Part 4.2 requires that entities verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. While entities consistently verified employees' recurring authorizations to

Electronic Security Perimeters (ESPs)[19] and Physical Security Perimeters,[20] entities did not always verify access to removable media in such reviews.

4. Review all firewalls to ensure there are no obsolete or overly permissive firewall access control rules in use.

Relates To

CIP-005-5 Requirement R1

Entities generally ensure that inbound and outbound access into an ESP is granted for specific business reasons and denied for all unneeded electronic access by default. Nonetheless, in a minority of instances, staff observed that entities maintained firewalls with overly permissive firewall access IP ranges. Examples include:

1. The use of overly broad IP ranges that include more IP addresses than applicable Cyber Assets; and
2. The assignments of Cyber Assets to an IP address within an IP range with access rights that was not designed for that Cyber Asset.

Maintaining overly permissive firewall access IP ranges increases the risk of malicious or otherwise harmful network traffic crossing an Electronic Access Point (EAP) into an ESP, which could harm reliable operation of the BES.[21] Firewall reviews should ensure IP ranges and their access rights are assigned to Cyber Assets appropriately.

5. Limit access to employee's PIN numbers used for accessing PSPs using a least-privilege approach.

[19] The NERC Glossary defines "Electronic Security Perimeter" as a logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

[20] The NERC Glossary defines "Physical Security Perimeter" as the physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

[21] The NERC Glossary defines an "Electronic Access Point" as a Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter. In most cases, this term can be generally or simply considered a "firewall."

Relates To

CIP-006-6 Requirement R1

Reliability Standard CIP-006-6, Requirement R1, Part 1.3 requires, for High Impact PSPs, "where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access." Entities commonly use a key card and PIN authentication as the two different physical access controls. However, some entities do not limit access to PIN numbers to the minimum number of necessary employees. For example, staff has observed some registered entities store their employee PIN numbers as plain text within the PACS management system and allow a broad range of employees (e.g., system operators or administrators) to have access to view the employee PIN numbers. This approach weakens the second physical access control, reducing overall security by allowing others to know an employee's PIN.

6. Ensure that all ephemeral port ranges are within the Internet Assigned Numbers Authority (IANA) recommended ranges.

Relates To

CIP-007-6 Requirement R1

Entities generally limited their ephemeral port ranges to eliminate unnecessary exposure to outside Cyber Assets.[22] However, in rare instances, an entity maintained a Cyber Asset with a broader than necessary ephemeral port range. An unnecessarily broad ephemeral port range increases the Cyber Asset's possible vulnerabilties to cyber attacks. Entities should have the least ephemeral

[22] An ephemeral port is a short-lived transport protocol port for Internet Protocol (IP) communications allocated automatically from a predefined range by a Cyber Asset's IP stack software. An ephemeral port is typically used as the port assignment for the client end of a client–server communication to a well-known port on a server, or on the server end of a communication it is used to continue communications with a client that initially connected to one of the server's well known port. Put another way, it allows two Cyber Assets to know who the other is when communicating.

port range that is necessary for their Cyber Assets. The Internet Assigned Numbers Authority[23] recommends a range of 49,152 to 65,535 for ephemeral ports.[24]

7. Clearly mark Transient Cyber Assets and Removable Media.

Relates To

CIP-010-2, Requirement R4

While entities generally only used Transient Cyber Assets[25] and Removable Media[26] to access BES Cyber Systems, staff observed several instances in which "unmanaged" Cyber Assets or storage media were used by accident.[27] In these instances, the entity's employee or contractor mistakenly used an unmanaged Cyber Asset or storage media believing that it was a Transient Cyber Asset or a Removable Media. Such errors unnecessarily expose a BES Cyber System to malicious code.

To minimize such inadvertent errors, entities could use color covers or distinctive labels for Transient Cyber Assets and Removable Media. Additionally, entities could use customized log-in screens for Transient Cyber Assets.

---

[23] The Internet Assigned Numbers Authority (IANA) manages registries that are critical for the operation of the Internet, including the DNS Root, the global pool of IP addresses, and the Internet protocols developed by standard bodies.

[24] *See* "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry" at 10. Found here: https://tools.ietf.org/html/rfc6335.

[25] The NERC Glossary defines a "Transient Cyber Asset" as a Cyber Asset that is: (1) capable of transmitting or transferring executable code; (2) not included in a BES Cyber System; (3) not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems; and (4) directly connected (*e.g.*, using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or PCA associated with high or medium impact BES Cyber Systems. Often this is a laptop used to perform maintenance on a BES Cyber System.

[26] The NERC Glossary defines "Removable Media" as storage media that: (1) are not Cyber Assets, (2) are capable of transferring executable code, (3) can be used to store, copy, move, or access data, and (4) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to: floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

[27] Reliability Standard CIP-010-2, Requirement R4 requires Transient Cyber Assets and Removable Media to be "managed" according to the sections of Reliability Standard CIP-010-2, Attachment 1.

VI. Previous Lessons Learned Recommendations

Below are the recommendations from the 2018 Lessons Learned Report and the 2017 Lessons Learned Report.

A. 2018 Lessons Learned[28]

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 enough to ensure proper authentication of internal connections.
3. Consider implementing encryption for Interactive Remote Access (IRA) that is sufficiently strong enough 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 (ICMP) 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.

B. 2017 Lessons Learned[29]

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

---

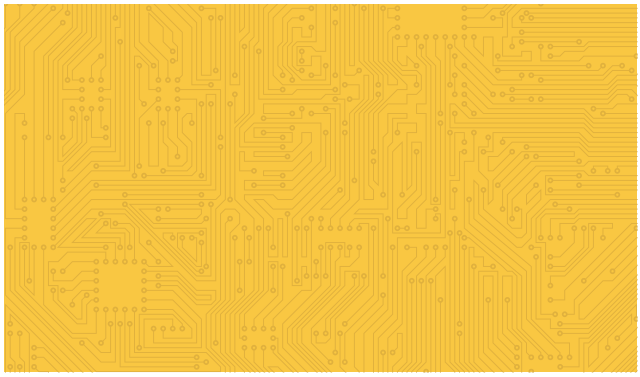
28 *See* 2018 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits (Feb. 6, 2018), https://www.ferc.gov/legal/staff-reports/2019/2018-report-audits.pdf.

29 *See* 2017 Staff Report Lessons Learned from Commission-Led CIP Version 5 Reliability Audits (Oct. 6, 2017), https://www.ferc.gov/legal/staff-reports/2017/10-06-17-CIP-audits-report.pdf.

or where inconsistencies exist between documents; and modify documentation accordingly.

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 Physical Security Perimeter (PSP).
8. 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.
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 EAPs exist.
12. Review all firewall rules and ensure access control lists follow the principle of "least privilege."
13. 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.
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 BES Cyber System Information (BSCI) storage evaluation procedures.

20. 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."
21. Document all procedures for the proper handling of BCSI.



2018 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits

Staff Report
Federal Energy Regulatory Commission
October 2019