

2020 Staff Report

# Lessons Learned from Commission-Led CIP Reliability Audits



**2020 Staff Report**  
**Lessons Learned from  
Commission-Led  
CIP Reliability Audits**

---



Prepared by Staff of the  
**FEDERAL ENERGY REGULATORY COMMISSION**  
Washington, D.C.

October 2, 2020

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.

# Contents

<b>I.</b>	<b>Introduction.....</b>	<b>1</b>
<b>II.</b>	<b>CIP Reliability Standards.....</b>	<b>2</b>
<b>III.</b>	<b>Audit Scope and Methodology.....</b>	<b>3</b>
<b>IV.</b>	<b>Overview of Lessons Learned.....</b>	<b>5</b>
<b>V.</b>	<b>Lessons Learned Discussion .....</b>	<b>6</b>
<b>VI.</b>	<b>Previous Lessons Learned Recommendations .....</b>	<b>13</b>
	A. 2019 Lessons Learned.....	13
	B. 2018 Lessons Learned.....	13
	C. 2017 Lessons Learned.....	14

# I. Introduction

During Fiscal Year (FY) 2020,<sup>1</sup> staff of the Federal Energy Regulatory Commission (Commission) completed non-public Critical Infrastructure Protection (CIP) audits (CIP Audits) of several “registered entities”<sup>2</sup> of the bulk electric system (BES).<sup>3</sup> The CIP Audits evaluated registered entities’ compliance with the applicable Commission-approved CIP Reliability Standards.<sup>4</sup> 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 required by the CIP Reliability Standards. Therefore, this report includes recommendations regarding cyber security practices that are voluntary.

This anonymized summary report informs the regulated community and the public of lessons learned from the FY20 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.

---

<sup>1</sup> 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 2020 begins on October 1, 2019 and ends on September 30, 2020.

<sup>2</sup> All Bulk-Power System users, owners and operators are required to register with NERC and, once registered, are commonly referred to as “registered entities.”

<sup>3</sup> BES is defined in the “Glossary of Terms Used in NERC Reliability Standards” (NERC Glossary), [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf) (June 2, 2020).

<sup>4</sup> 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 (2020).

## 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.<sup>5</sup> 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,<sup>6</sup> and subsequently certified NERC.<sup>7</sup> 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 cyber 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 cybersecurity.<sup>8</sup> 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 cyber security CIP Reliability Standards audits of registered entities of the BES in FY16, and the Commission has conducted CIP audits each year since FY16.

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-003-8](#) – 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-009-6](#) – Recovery Plans for BES Cyber Systems
9. [CIP-010-2](#) – Configuration Change Management and Vulnerability Assessments
10. [CIP-011-2](#) – Information Protection

---

<sup>5</sup> 16 U.S.C. 824o (2012).

<sup>6</sup> *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).

<sup>7</sup> *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).

<sup>8</sup> *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).

### 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<sup>9</sup> identified by an entity as High, Medium, or Low Impact;<sup>10</sup> 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<sup>11</sup> and Protected Cyber Assets<sup>12</sup> within a BES Cyber System<sup>13</sup> or associated Cyber Assets mainly, but not always, outside the BES Cyber System (*i.e.*, Electronic Access Control or Monitoring Systems (EACMS)<sup>14</sup> and Physical Access Control Systems (PACS)<sup>15</sup>).

---

<sup>9</sup> The NERC Glossary defines "Cyber Assets" as programmable electronic devices, including the hardware, software, and data in those devices.

<sup>10</sup> 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.

<sup>11</sup> 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.

<sup>12</sup> 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.

<sup>13</sup> 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.

<sup>14</sup> The NERC Glossary defines Electronic Access Control or Monitoring Systems (EACMS) as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." 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.

<sup>15</sup> The NERC Glossary defines Physical Access Control Systems (PACS) as "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers."

## 2020 REPORT ON CIP AUDITS

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 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 intended to help responsible entities improve their compliance with the CIP Reliability Standards and their overall cyber security posture:

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 electronic access to BES Cyber System Information (BCSI) 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 Physical Security Perimeters (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. Consider evaluating the security controls implemented by third parties regularly and implement additional controls where needed when using a third party to manage BES Cyber System Information (BCSI).

## V. Lessons Learned Discussion

1. Ensure that all BES Cyber Assets are properly identified.

**Required By  
CIP-002-5.1a R1**

While entities generally identified BES Cyber Assets effectively, in some cases entities did not identify BES Cyber Assets equipment performing supporting functions. For example, several entities misidentified Cyber Assets as communications equipment instead of BES Cyber Assets. Cyber Assets that seem to serve only a communication function such as switches and protocol converters may pose an impact to the BES within 15 minutes of their misuse. NERC, in a lessons learned document, recommends assessing whether all Cyber Assets can impact the BES within 15 minutes including communication Cyber Assets.<sup>16</sup>

Though not required by the CIP Reliability Standards, entities should consider the guidance of the National Institute of Standards and Technology (NIST) Technical Guide to Information Security Testing and Assessment, and the Configuration Management control family of NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53).<sup>17</sup> For example, periodic enterprise-wide network mapping, baselining and diligent discovery activity are crucial to the development of an accurate network diagram to facilitate incident detection, response, and recovery operations.

2. Ensure that all substation BES Cyber Systems are properly categorized as high, medium, or low impact.

**Required By  
CIP-002-5.1a R1  
Attachment 1  
Criterion 2.5**

While entities generally categorized the impact rating of BES Cyber Systems associated with substations effectively and accurately, in some cases entities did not properly consider the interdependency of relay schematics and configurations between control houses containing separate voltage levels. This can lead to the misidentification of a BES Cyber System located at a substation as low impact instead of medium impact. For example, 138 kV breaker failure relays can trip 345 kV buses, and as a result can impact 345 kV BES Cyber Systems classified as medium impact. In such circumstances, the Cyber Assets associated with the 138 kV breaker failure relays should also be categorized as medium impact BES Cyber Systems.

<sup>16</sup> NERC, “Lesson Learned CIP Version 5 Transition Program, Communications to BES Cyber Systems and Cyber Assets”; <https://www.nerc.com/pa/CI/tpv5impmntnsty/External%20Routable%20Connectivity%20Lesson%20Learned.pdf>

<sup>17</sup> National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 (NIST SP 800-53) is a publication developed by NIST as part of its statutory responsibilities establishing information security standards and guidelines, including minimum requirements for federal information systems. Found here: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

3. Ensure that electronic access to BES Cyber System Information (BCSI) is properly authorized and revoked.

**Required By**  
**CIP-004-6**  
**Requirements R4 & R5**

In general, entities appropriately authorized electronic access; and access to designated electronic storage locations, for BCSI.<sup>18</sup>

However, some entities did not consistently apply their documented process(es) to properly authorize, or in cases of termination, revoke, employees' access to BCSI. Specifically, some entities failed to follow

their documented processes to:

1. Authorize electronic access to designated storage locations for BCSI. For example, in some instances access was granted to electronic BCSI storage locations in a manner that differed from the entity's documented program, including instances where verbal approval for access was granted without maintaining the necessary documentation required by its procedures.
2. Remove a terminated employee's access to BCSI storage locations by the end of the next calendar day. In some instances, entities collected an individual's physical badge by the end of the next calendar day but did not deactivate the user network accounts in a timely manner. As a result, the dormant account and its associated access privileges remained on the network for an extended period beyond the next calendar day, presenting an attack vector that could be used to mimic a legitimate employee.

Overly permissive or inaccurate electronic access rights to BCSI, as well as unauthorized access, increases the risk of inappropriate release of information that could lead to compromise and/or mis-operation of BES Cyber Systems.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the Access Control (AC) family of NIST SP 800-53. For example, according to NIST SP 800-53 all Access Control Lists (ACLs) should include third-party vendors. In addition, entities should consider automated control mechanisms for managing the creation, access, disablement, and archiving of accounts.

---

<sup>18</sup> The NERC Glossary defines "BES Cyber System Information" as "information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System."

4. Consider having a dedicated visitor log at each Physical Security Perimeter (PSP) access point.

**Relates To**  
**CIP-006-6 Requirement R1**

Certain entities share a single visitor log between multiple access points within a single PSP, which necessitates moving the log back and forth between access points.<sup>19</sup> Such movements could decrease the security posture for protecting the PSP.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the Physical and Environmental Protection (PE) family of the NIST SP 800-53, specifically as it relates to visitor access records. For example, PE-8 recommends that, for high impact information systems, entities employ automated mechanisms to facilitate the maintenance and review of visitor access records.

5. Consider locking BES Cyber Systems' server racks where possible.

**Relates To**  
**CIP-006-6 Requirement R1**

Entities' server racks located in their control centers and substations typically have the capability to be locked.<sup>20</sup> Yet, not all entities consistently use this capability.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the PE control family of the NIST SP 800-53, as it relates to physical access control. For example, it is important for the entity to regulate and limit access to resources to reduce the risk of data theft and disruption. In addition to maintaining servers in lockable casings, entities should determine who should have access to servers and define procedures for visitor and third-party escorts and monitoring.

6. Inspect all Physical Security Perimeters (PSPs) periodically to ensure that no unidentified physical access points exist.

**Required By**  
**CIP-006-6 Requirement R1**

In general, entities properly identified all access points to their PSPs. However, some entities did not consider access points, often in the ceilings or other locations, that are large enough for a person to gain access to the PSP, such as maintenance access points.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the PE family of the NIST SP 800-53 in making such identifications. For example, entities should consider

---

<sup>19</sup> 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.

<sup>20</sup> A server rack, usually located in data centers or communications closets, is a piece of equipment that houses Cyber Assets, such as switches, network appliances, and servers.

installing physical boundaries addressing all access points to secure spaces related to overhead compartments.

7. Review security patch management processes periodically, and ensure that they are implemented properly.

**Required By**  
**CIP-007-6, Requirement R2**

Some entities did not have a consistent security patch management process for applicable Cyber Assets. Staff observed potential risks and areas for improvement in security patch management related to: (1) understanding the proper scope of security patch applicability, (2) procedures for tracking applicable security patches, and (3) controls

to ensure all applicable security patches are installed or a mitigation plan is in place.

- Staff observed some entities made security patch implementation decisions based on the risk of exploitation of the vulnerability. The risk of exploitation of a vulnerability is not a factor in determining the application of a security patch. All identified security patches must be evaluated and then either applied or mitigated.
- Some entities did not have clearly delineated procedures for tracking applicable security patches and lacked consistency between the procedures used by their business units. Staff observed that, due to such “siloeing” among work units, some entities’ procedures lacked clear steps for tracking patches and mitigation plans for third-party applications. If security patches are not accounted for through mitigation plans, security vulnerabilities could be exploited in a malicious manner to gain control of a BES Cyber Asset or BES Cyber System or render the BES Cyber Asset or BES Cyber System inoperable.
- In other cases, entities lacked adequate controls to ensure that all security patches were installed. Staff observed that these issues occurred where entities employed manual tracking processes that were labor-intensive and presented a higher risk of human error. To improve patch management processes, entities should consider additional controls, such as automated methods where possible, and enhanced quality assurance methods where manual methods are still used.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the NIST SP 800-40 Guide to Enterprise Patch Management Technologies and the Audit and Accountability (AU) control family of NIST SP 800-53. For example, entities should consider an automated information system for system patching efforts. In addition, actions implemented to mitigate identified vulnerabilities should be periodically audited to ensure alignment with approved network baselines, access management protocols, and entity risk tolerance factors.

8. Consider consolidating and centralizing password change procedures and documentation.

**Relates To**  
**CIP-007-6, Requirement R5**

Entities generally implemented sufficient password change procedures. However, entities that did not use a centralized password database encountered difficulties tracking and monitoring password changes. Entities that primarily relied on databases and spreadsheets to implement password change processes and procedures frequently did not include in their accounts all applicable Cyber Assets requiring procedural password changes. To obtain detail at the applicable Cyber Asset level, entities relied on multiple different sources to track and monitor password change activity. The requirement to change passwords exists primarily to address password cracking attempts. Failure to properly track and document password changes presents the risk that accounts may be missed during password changes, which increases the likelihood of compromised passwords.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the Identification and Authentication (IA) control family of NIST SP 800-53. For example, entities should consider automated auditing of accounts and implementing access control measures on all centralized password repositories.

9. Ensure that backup and recovery procedures are updated in a timely manner.

**Required By**  
**CIP-009-6, Requirement R1**

While entities generally maintained documented processes for the backup and storage of information required to recover BES Cyber System functionality as required in CIP-009-6, R1.3, some entities failed to update their backup and recovery procedures in a timely manner. In some cases, entities responded to a critical event which required the entity to establish a new process that differed from their documented procedure. In these cases, the entities continued to use the new process without updating their documented process or procedure.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the Contingency Planning (CP) control family of NIST SP 800-53. For example, entities should consider systematic preservation of system documentation.

10. Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.

**Required By**  
**CIP-010-2, Requirement R3**

Some entities did not report any information to remediate or mitigate vulnerabilities identified in vulnerability assessments, including the planned date of completing the action plan and the execution of any remediation of mitigation items as required by CIP-010-2, Requirement R3, Part 3.4. The vulnerability assessment process is one component in an overall program to periodically ensure the proper implementation of cyber

security controls, as well as to continually improve the security posture of BES Cyber Systems.<sup>21</sup> Failure to thoroughly document the assessment and subsequent analysis and remediation or mitigation activities could undermine this intent.

Entities should consider incorporating the following elements into an entity’s vulnerability assessment process for all Cyber Assets: network port and service identification, network discovery and wireless review, as set forth in NERC CIP-010-2 Guidelines and Technical Basis. Though not required by the CIP Reliability Standards, entities should also consider the guidance of NIST SP 800-115 Technical Guide to Information Security Testing and Assessment. For example, upon completion of a vulnerability scan, entities should generate a report. The report should identify system and network vulnerabilities and appropriate mitigation actions.

11. Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.

**Required By**  
**CIP-011-2, Requirement R2**

Some entities were unable to demonstrate that they properly disposed of all devices removed from service at substations in accordance with the entities’ documented process. In one instance, staff observed that although an entity maintained a strong documented information protection program, it failed to document and track some substation devices removed from service. Entities could improve their asset tracking procedures by ensuring that they maintain asset reuse and disposal logs for all substation assets that are referenced in documented procedures. Failure to properly track the reuse and disposal of substation assets could lead to the improper release or unauthorized retrieval of BCSI contained on the devices.

Though not required by the CIP Reliability Standards, entities should consider the guidance of the Media Protection (MP) control family of NIST SP 800-53, as it relates to media sanitization. For example, entities should develop full testing and verification procedures for sanitized storage devices designated for system reuse and consider the use of two-party verification of all sanitization actions.

12. Consider evaluating the security controls implemented by third parties regularly, and implement additional controls where needed when using a third party to manage BES Cyber System Information (BCSI).

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

Entities generally implemented sufficient procedures and controls to properly protect and securely handle BCSI, including while in storage, transit, and use. However, some entities relied solely on security controls provided by third-party vendors without first verifying that these controls are sufficient. Failure to ensure the sufficiency of third-party vendor controls

---

<sup>21</sup> See CIP-010-2, Guidelines and Technical Basis, Rationale at page 44.

## 2020 REPORT ON CIP AUDITS

could create a risk of compromise to the BCSI if the third-party vendor controls do not provide the necessary level of protection.

Entities should perform due diligence to ensure that the selected third-party vendors use sufficient security controls. Though not required by the CIP Reliability Standards, entities should consider guidance from NIST SP 800-35 “Guide to Information Technology Security Services,” which recommends that the customer take responsibility for identifying and implementing all security controls required to protect data both in transit and at rest when employing third-party contractors. Further, NIST SP 800-35 recommends that most cloud services and third-party vendors add specific contractual clauses releasing them from responsibility for data breaches. To mitigate risks, entities should inspect third-party vendors’ existing security controls and supplement, as necessary, based on data sensitivity, encryption requirements, and existing access controls.

## VI. Previous Lessons Learned Recommendations

### A. 2019 Lessons Learned<sup>22</sup>

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.

### B. 2018 Lessons Learned<sup>23</sup>

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 (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.

---

<sup>22</sup> See 2019 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits (Oct. 4, 2019), [https://www.ferc.gov/sites/default/files/2020-05/2019-report-audits\\_0.pdf](https://www.ferc.gov/sites/default/files/2020-05/2019-report-audits_0.pdf)

<sup>23</sup> 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](https://www.ferc.gov/sites/default/files/2020-05/2018-report-audits_0.pdf)

## C. 2017 Lessons Learned<sup>24</sup>

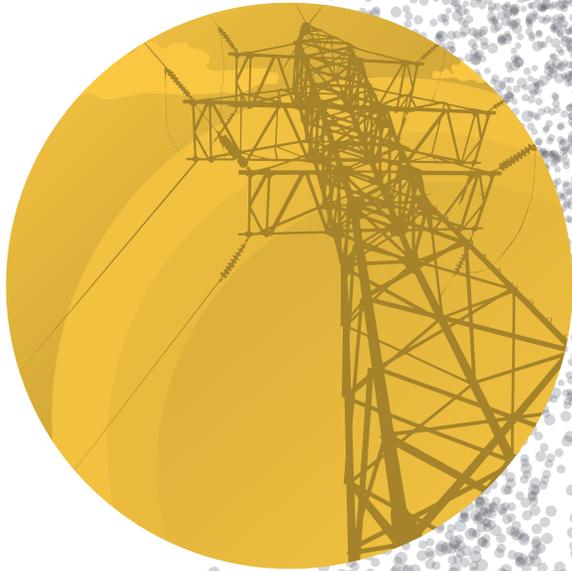
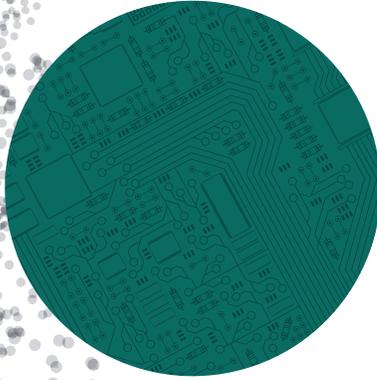
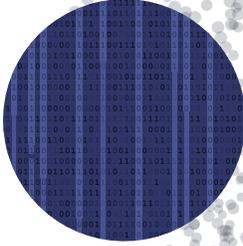
1. Conduct a thorough review of CIP Reliability Standards compliance documentation; identify areas of improvement to include but not be limited to instances where the documented instructional processes are inconsistent with actual processes employed or where inconsistencies exist between documents; and modify documentation accordingly.
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.

---

<sup>24</sup> 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](https://www.ferc.gov/sites/default/files/2020-05/10-06-17-CIP-audits-report_0.pdf).

## 2020 REPORT ON CIP AUDITS

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 (CIPC) guidance document, “Security Guideline for the Electricity Sector: Protecting Sensitive Information.”
21. Document all procedures for the proper handling of BCSI.



2020 Staff Report  
**Lessons Learned  
from Commission-Led  
CIP Reliability Audits**

