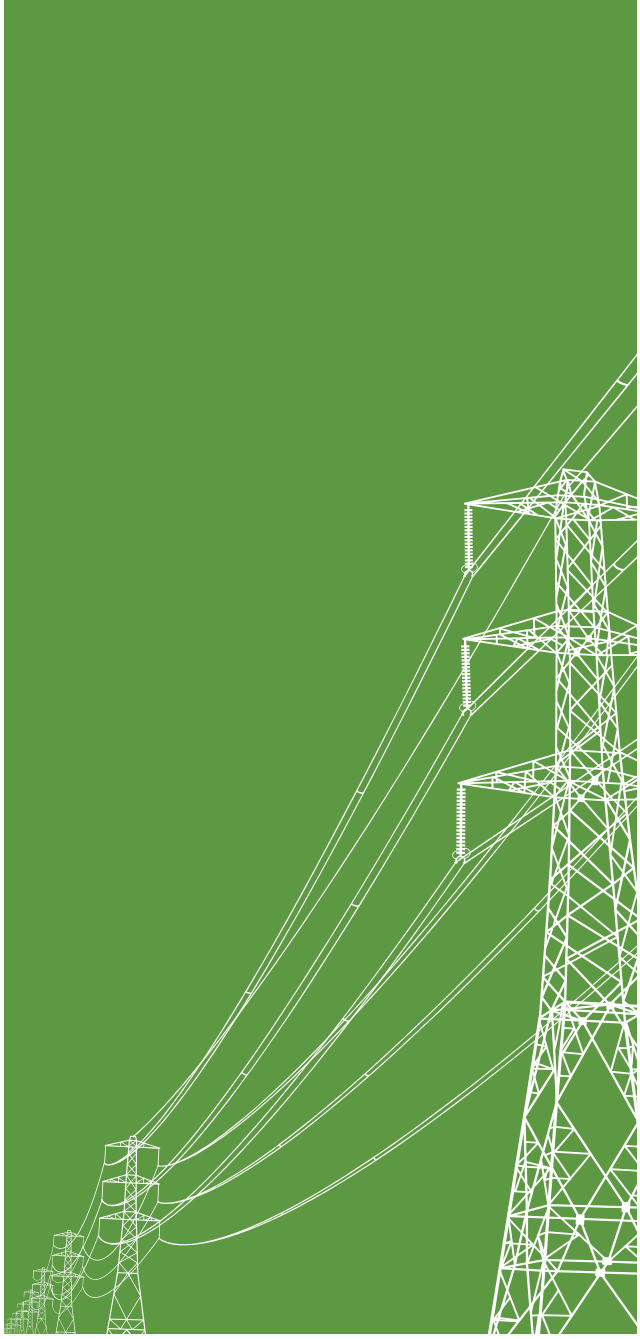
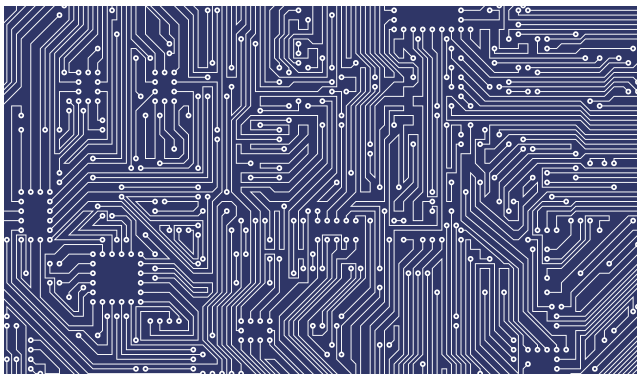




2018 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits

Staff Report
Federal Energy Regulatory Commission
March 2019

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

2018 Staff Report
Lessons Learned from Commission-Led CIP Reliability Audits

Prepared by Staff of the
Federal Energy Regulatory Commission

Washington, D.C.

March 29, 2019

Table of Contents

Introduction

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".[1] of the Bulk Electric System (BES).[2] The audits evaluated registered entities' compliance with the applicable Commission-approved CIP Reliability Standards.[3] Staff from Regional Entities and the North American Electric Reliability Corporation (NERC) participated in the audits, including the on-site portion. The audits were completed for Fiscal Years 2016 through 2018 (FY16, FY17, and FY18).[4]

During the 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 noted observations of 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

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

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

[3] 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 (2018).

[4] 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 2018 begins on October 1, 2017 and ends on September 30, 2018.

[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.

observations derived from audits carried out in FY16 and FY17 was shared with the industry in the 2017 Lessons Learned Report.[6]

These CIP Audits were non-public. This anonymized summary report informs the regulated community and the public of additional lessons learned from the FY18 audits. This report provides information and recommendations to NERC, regional entities, and registered entities that staff believes are useful in their assessments of risk, 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.

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.[7] 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,[8] and subsequently certified NERC.[9]

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.[10] 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 CIP Reliability Standards are designed to mitigate the cybersecurity 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.

[7] 16 U.S.C. 824o (2012).

[8] *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).

[9] *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).

[10] *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).

Audit Scope and Methodology

The Commission initiated its CIP Reliability Standards audits of registered entities of the BES in FY16. The audits focused on evaluating compliance with CIP Reliability Standards version 5 for periods after July 1, 2016.[11] The Commission also evaluated compliance with CIP Reliability Standards version 3 (CIP v3), for the period of each audited entity's last CIP compliance audit through June 30, 2016 (the effective end date of CIP v3).[12]

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[13] identified by an entity as High, Medium, or Low Impact;[14] and interviewed compliance program managers, staff, and employees responsible for day-to-day compliance and regulatory oversight.

---

[11] *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.

[12] *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.

[13] The NERC Glossary defines Cyber Assets as programmable electronic devices, including the hardware, software, and data in those devices. Applicable Cyber Assets consists of BES Cyber Assets and Protected Cyber Assets within a BES Cyber System or associated Cyber Assets outside the BES Cyber System (*i.e.*, EACMS and PACS).

[14] The CIP Reliability Standards requires 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.

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.

Overview of Lessons Learned

The lessons observed and discussed in this report are derived from the FY18 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.

Of note, there were some lessons observed and discussed in this report that were also detected in prior years and included in the 2017 Lessons Learned Report. Staff believes that continued attention to such matters will foster greater recognition toward compliance with the CIP Reliability Standards throughout the industry. As such, some previous lessons from the 2017 Lessons Learned Report are included with new additional information. Where appropriate, staff have indicated specific requirements to which the lessons learned could pertain.

New Lessons Learned

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 Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (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.

Previous Lessons Learned

11. Conduct a thorough review of CIP Reliability Standards compliance documentation to identify where the documented instructional processes are inconsistent with actual processes employed.

12. For each remote cyber asset conducting IRA, disable all other network access outside of the connection to the applicable Cyber System that is being remotely accessed, unless there is a documented business or operational need.
13. Enhance documented processes and procedures for identifying BES Cyber System Information to consider the NERC Critical Infrastructure Protection Committee guidance document, "Security Guideline for the Electricity Sector: Protecting Sensitive Information."

New Lessons Learned Discussion

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.

Relates To

CIP-004-6 Table R1 Security Awareness Program

While entities generally implemented strong plans and processes regarding their security awareness programs, the documentation addressing training-needs assessment could be improved. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50 states that an entity should: (1) identify what awareness, training, and/or education are needed; (2) identify the current efforts to address those needs; (3) analyze the effectiveness of those current efforts; (4) identify all gaps between the needs and what is being done; and (5) assess which needs are the most critical.[15]

In some instances, an entity's security awareness programs documentation did not provide sufficient procedures or policies to analyze the effectiveness of the entity's security awareness program. For example, some entities did not track if and when an employee or contractor viewed a video regarding cybersecurity practices. This resulted in those entities falling short of addressing all of the recommendations from the NIST 800-50 publication.

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.

Relates To

CIP-005-5 Requirement R1 Electronic Security Perimeter and
CIP-007-6 Requirement R5 System Access Control

Some entities did not use Security Certificates when accessing web servers internal to the BES Cyber System, or the Security Certificates that are being used are either expired or using outdated encryption.[16] The result is the generation of an error message for the user. Generally, the security risks associated with certificate errors are

[15] NIST SP 800-50 Section 3.2; "Building an Information Technology Security Awareness and Training Program" at 18; found here: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.

[16] Security Certificates are files that ensures secure communication via a cryptographic key from a web server to a browser. Web browsers visually show whether a web server is secure, and commonly warn the person using the browser if he/she is connecting to a web server that does not utilize a Security Certificate. Security Certificates have a validity period usually capped at two years. Security Certificates employ

minimal when all of the accessed cyber assets are located solely within a BES Cyber System. However, a user may become accustomed to allowing the continuation of a connection with a Security Certificates error, and thus may become desensitized to the error message.

It is common for a user within a BES Cyber System to access approved web servers both internal and external to the BES Cyber System. The external connections should almost always use Security Certificates. The concern is that in situations where internal web servers are not required to have Security Certificates, and there is an actual security certificate error with an external connection, the user may out of habit accept the external connection with the error.

The Electronic Security Perimeter (ESP) limits reconnaissance of targets, restricts and prohibits traffic, and assists in containing any successful attack.[17] Thus, the ESP provides a first layer of cyber security defense in depth for network-based attacks. Users desensitized to security certificate errors could undermine the effectiveness of ESP(s).

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.

Relates To

CIP-005-5 Requirement R2 Interactive Remote Access Management

While most audited entities implemented encryption for IRA[18] that was sufficiently strong enough to protect the data that is sent between the remote access client and the BES Cyber System's Intermediate System,[19] several entities used the

cryptographic algorithms to encrypt communication which may become outdated. For example, the SHA-1 algorithm is no longer trusted by the Chrome web browser.

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

[18] The NERC Glossary defines IRA as user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's ESP(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

[19] The NERC Glossary defines an Intermediate System as a Cyber Asset or collection of Cyber Assets performing access control to restrict IRA to only authorized

Intermediate System's default "lower" encryption strength.[20] These entities could increase their encryption strength for IRA with a simple configuration setting of their Intermediate System, without having to purchase new hardware or software.

4. Consider Internet Control Message Protocol (ICMP) as a logical access port for all the BES Cyber Assets.

Relates To
CIP-007-6 Requirement R1
Ports and Services

While entities generally had adequate security controls to identify and protect ICMP[21] communications at the network or BES Cyber System level, some entities did not identify and protect ICMP communications at the host, or Cyber Asset level. While not a requirement of the CIP Reliability Standards, disabling all ICMP communication for any Cyber Asset that does not have a business need for ICMP improves an entity's cybersecurity posture.

5. Enhance documented processes and procedures for incident response to consider the NIST SP 800-61, "Computer Security Incident Handling Guide."

Relates To
CIP-008-5
Incident Reporting and
Response Planning

While entities generally implemented effective plans and processes for incident response, documentation differentiating the policies, plans, and procedures could be improved.

NIST SP 800-61 states that an entity's: (1) incident response policy should include objectives, prioritization, organizational structure, and performance measures regarding entity's handling of security incidents; (2) incident response plan should include the formal organizational approach to incident response, communication protocols while processing the incident response, and metrics for measuring incident response capability; and (3) incident response procedures should be based on the incident response policy and plan and

---

users. The Intermediate System must not be located inside the Electronic Security Perimeter.

[20] Encryption strength is a measure of the key size (number of bits in the key) used to encrypt data. For example, the NIST AES specification has three different key lengths: 128, 192, and 256 bits, from weakest to strongest.

[21] ICMP is a supporting protocol of the Internet protocol suite used primarily to deliver error messages to Internet Protocol (IP) users and to perform network diagnostics. ICMP Echo-request/reply, commonly known by the command "Ping," is a way to query a network's systems to find out if a host is live on a network.

should include "standard operating procedures, of the specific technical processes, techniques, checklists, and forms used by the incident response team."[22]

In some circumstances, the distinction between an entity's incident response policy, plan, and procedure was unclear. Meaningful distinctions could enhance an entity's implementation of the NIST SP 800-61 recommendations.

6. Consider the remote configuration of applicable Cyber Assets via a TCP/IP-to-RS232 Bridge during vulnerability assessments.

Relates To

CIP-010-2 Requirement R3 Vulnerability Assessments

Entities may have applicable Cyber Assets connected to a routable network via a TCP/IP-to-RS232 Bridge that can be configured remotely. While entities generally had security controls to protect such applicable Cyber Assets, the vulnerability assessments for these applicable Cyber Assets could be improved. For example, some entities did not identify which applicable Cyber Assets could or could not be configured remotely. By ensuring an examination of an applicable Cyber Assets remote configuration via TCP/IP-to-RS232 Bridge in an entity's vulnerability assessments, an entity's overall cyber security posture could be improved.

7. Consider the use of Secure Administrative Hosts to perform administrative tasks when accessing either Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS).

Relates To

All CIP Reliability Standards Applicable to Associated Cyber Assets of BES Cyber Systems

Administrative hosts are Cyber Assets used by system administrators[23] to access Electronic Access Control or Monitoring Systems (EACMS)[24] or

[22] *See* SP 800-61 Rev. 2 Section 2.3.3; "Computer Security Incident Handling Guide"; found here: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[23] System administrators, or sysadmins, are users with privileged accounts who are responsible for the configuration, operation, and security of cyber assets or cyber systems.

[24] The NERC Glossary defines Electronic Access Control Monitoring Systems as Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This definition includes

Physical Access Control Systems (PACS).[25] While the CIP Reliability Standards addresses applicable Cyber Assets, the administrative hosts used to access those associated cyber assets are not always addressed by the CIP Reliability Standards. Entities should consider the use of stringent security controls, such as those required by the CIP Reliability Standards for applicable Cyber Assets, for these administrative hosts. Administrative hosts that received specialized security controls are sometimes referred to as "Secure Administrative Hosts."[26]

8. Consider replacing or upgrading "End-of-Life" system components of an applicable Cyber Asset.

Relates To

CIP-007-6 Requirement R2 Security Patch Management and CIP-010-2 Requirement R1 Configuration Change Management

While entities generally ensured all applicable security patches were installed for the release version of a BES Cyber Asset's system component (*e.g.*, software, firmware, or hardware), not all entities were using the most current release of a BES Cyber Asset's system component.[27] In some cases, entities used a system component that

Intermediate Systems. Examples of EACMS are Active Directory or other types of directory services servers.

[25] The NERC Glossary defines Physical Access Control Systems 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.

[26] Secure Administrative Hosts are similar in concept as secure administrative workstations (SAWs) or dedicated administrative workstations. For Windows-based Secure Administrative Hosts, Microsoft has published a guide on how to implement such hosts as secure administrative host. See Microsoft "Implementing Secure Administrative Hosts"; at: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts.

[27] Although security patches are mostly associated with software, and to a lesser degree firmware, hardware can also receive security patches. Modern Central Processing Units (CPUs) utilize "microcode" within the CPU that is loaded when the CPU boots. That microcode can receive security patches.

had reached the vendor's "end-of-life" date.[28] Such entities are at a higher risk for a cyber incident by not using the current release.

While the CIP Reliability Standards do not require entities to upgrade to new releases, it is a cybersecurity best practice to avoid using "unsupported system components."[29]

9. Consider incorporating file verification methods, such as hashing, during manual patching processes and procedures, where appropriate.

Relates To

CIP-007-6 Requirement R2
Security Patch Management

Entities generally verified the authenticity of manually downloaded patches and updates, usually by hashing. However, file verification was not employed consistently. A software hashing program uses a specific algorithm to produce a unique representative value of any file. This hash value can then be compared to the hash value that the vendor associated with a downloaded file to confirm that the downloaded file is authentic. Most vendors provide hash values of their patches and updates.[30]

NIST promotes verifying the authenticity of manually downloaded patches and updates.[31]

[28] A system component (*e.g.*, software, firmware, or hardware) "end-of-life" date is when the system component's vendor stops manufacturing spare parts, providing technical support, and/or providing new security patches for the component.

[29] *See* NIST SP 800-53 (Rev. 4), SA-22 "Unsupported System Components," which states that the entity should "(a). Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and (b). Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs."

[30] *See* Department of Homeland Security's National Cybersecurity and Communications Integration Center "File Hashing"; at: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_Factsheet_File_Hashing_S508C.pdf.

[31] *See* NIST SP 800-53 (Rev. 4), SI-7 "Software, Firmware, and Information Integrity," which states that the entity should "implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information."

10. Consider using automated mechanisms that enforce asset inventory updates during configuration management.

Relates To

CIP-010-2 Table R2 Configuration Monitoring

Entities generally maintained accurate up-to-date configuration baselines. However, some entities' configuration baselines were not accurate due to approved configuration changes that were not incorporated into the configuration baselines. Those entities typically did not incorporate configuration changes into baselines due to overlooking a manual component of the workflow process.

NIST recommends that entities "employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available [1] baseline configuration of the information system,[32] [and 2] inventory of information system components."[33]

[32] *See* NIST SP 800-53 (Rev. 4), CM-2(2) "Baseline Configuration - Automation Support for Accuracy."

[33] *See* NIST SP 800-53 (Rev. 4), CM-8(2) "Information System Component Inventory - Automated Maintenance."

Expanded Previous Lessons Learned Discussion

11. Conduct a thorough review of CIP Reliability Standards compliance documentation to identify where the documented instructional processes are inconsistent with actual processes employed.

Relates To

All CIP Reliability Standards

For audit evidence collection, Commission staff uses NERC's CIP evidence request process.[34] Staff has observed that often an entity's CIP documentation could be improved. Entities that review their CIP Reliability Standards compliance documentation to identify lack of completeness or accuracy often can also identify where their cyber security program might be deficient and could be improved. Suggestions for things to look for include the following:

- Do not leave required fields blank when the field is not applicable for a specific record, especially in baselines. State either "N/A" or "none" as appropriate.
- For any plan, process, or procedure addressing any sort of mitigation, be as concise and specific as possible regarding the compensating measures addressing the vulnerability.
- For any testing of an entity's incident response plan, ensure that the plan, process or procedure includes sufficient documented analysis regarding the effectiveness of testing. All deviations to the testing procedures determined from such analysis should be clear and specific. For specific recommendations, please reference NIST Special Publication 800-53 (Rev. 4), Control IR-1 "Incident Response Policy and Procedures."

12. 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.

Relates To

CIP-005-5 Requirement R2 Interactive Remote Access Management

Most entities' practice for conducting IRA allows other network communications to be made by the remote cyber asset conducting the IRA session. No current CIP Reliability Standard requirement directly limits other network communications on a remote cyber asset conducting an IRA. Limiting all other connections to the BES Cyber System

[34] *CIP Version 5 Evidence Request User Guide*, Version 1.0 (2015). Found here: https://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/CIP%20Version%205%20Evidence%20Request_v1_0_bt.pdf.

minimizes the overall attack surface of the entity while conducting an IRA and enhances an entity's cyber security posture.

Disabling "other" network access would include:

(1) Disabling split tunneling if the IRA cyber asset is using a Virtual Private Network (VPN) to connect to an Intermediate System; or
(2) Disabling dual-homing if the IRA cyber asset has more than one network connection.

Disabling Split Tunneling

Entities are required to use encryption for all IRA sessions to an Intermediate System. This is often implemented by using a VPN. Although not all VPN software allows split tunneling, most of VPN software used by entities will allow VPN configuration to enable split tunneling. VPN split tunneling is when a cyber asset accesses two different networks at the same time, using the same or different network interfaces; the network using the VPN connection and one that does not. The network that does not use the VPN is often the interface that connects to the Internet.

VPN is often used to allow a cyber asset access to a corporate network for internal files or data. Using VPN in default mode could allow a cyber asset to access the Internet through the corporate network. In some cases, the Internet access might be too slow for effective use, or Internet access might be blocked. In such cases, the cyber asset might be configured to allow split tunneling. This would allow the internal files or data access, while allowing effective Internet access.

BES Cyber Systems have restrictive Internet access. While conducting IRA, a cyber asset might have limited Internet access. While there could be certain business needs that would require a cyber asset to have access to a BES Cyber System and the Internet simultaneously, entities should not configure their IRA VPN to allow split tunneling by default.

Disabling Dual-Homing

Historically, dual-homed cyber assets (*i.e.*, cyber assets that have more than one network interface) were often switches, routers, and firewalls, or other cyber assets used to build data communication networks (*e.g.*, the Internet). Laptops and desktop computers now often have two network interfaces, a wireless network interface and a wired network interface. Although it is common for such cyber assets to be configured by default as not to allow both network interfaces to be active at the same time, often these cyber assets will allow that configuration to be changed to allow both interfaces to be active.

13. Enhance documented processes and procedures for identifying BES Cyber System Information to consider the NERC Critical Infrastructure Protection Committee guidance document, "Security Guideline for the Electricity Sector: Protecting Sensitive Information."

Relates To

CIP-011-2 Requirement R1 Information Protection

Audited entities generally had security controls to identify and protect BES Cyber System Information.[35] Nonetheless, most entities' BES Cyber System Information programs could benefit from the guidance in the NERC Critical Infrastructure Protection Committee[36] document, "Security Guideline for the Electricity Sector: Protecting Sensitive Information."[37] To enhance their documented processes and procedures for identifying BES Cyber System Information, entities could consider incorporating the following from the guidance:

- Identification of sensitive information.[38]
- Having a documented method for responding to data loss events.[39]

[35] 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.

[36] NERC's Critical Infrastructure Protection Committee coordinates NERC's security initiatives and serves as an expert advisory panel to NERC in the areas of physical security and cybersecurity.

[37] *See* NERC's "Security Guideline for the Electricity Sector: Protecting Sensitive Information." Found Here: http://www.nerc.com/comm/CIPC/Protecting%20Sensitive%20Information%20Guideline%20Task1/Protecting%20Sensitive%20Information%20Guideline%20(PSIGTF).pdf.

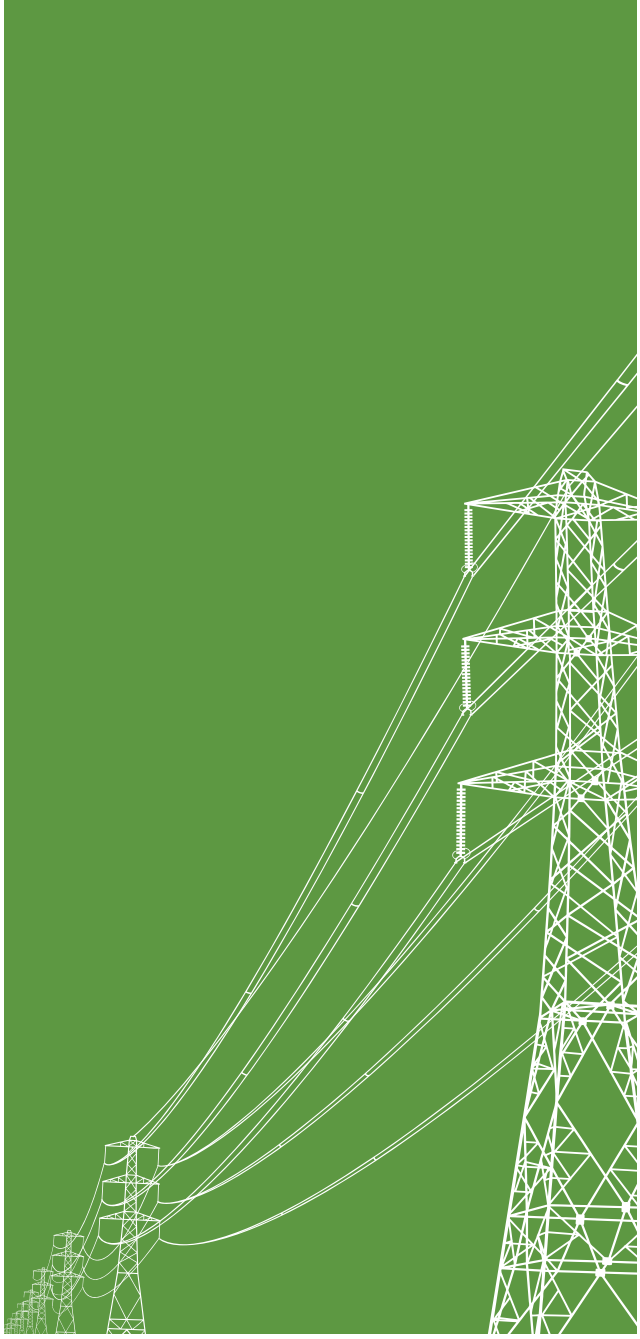
[38] *Id., see section:* "Identification of Sensitive Information" at 2.

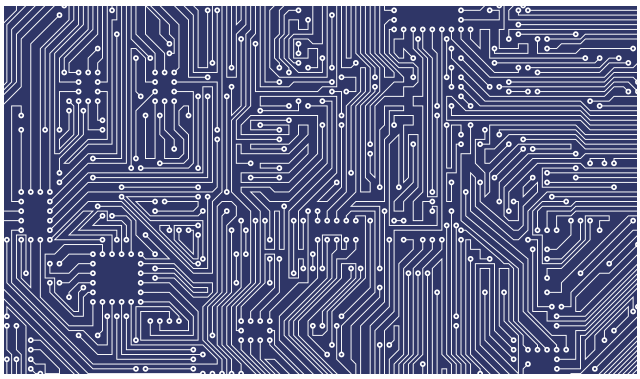
[39] *Id., see section:* "Responding to Inadvertent or Unauthorized Disclosures of Sensitive Information" at 11.

- Proper disposal of sensitive information.[40] The guidance document states that this information should be "digitally shredded" to ensure it cannot be recovered.[41]

[40] *Id., see subsection:* "Disposal" at 7.

[41] Within most cyber assets, deleting a file does not delete the file, rather it frees up the space that file was using. The actual data remains in the free space, until another file overwrites it during normal operation. Some digital forensic tools can even recover an original file that has been overwritten. "Digitally shredding" a file is writing over the file location multiple time to ensure that the original data underneath cannot be recovered.





2018 Staff Report

Lessons Learned from Commission-Led CIP Reliability Audits

Staff Report
Federal Energy Regulatory Commission
March 2019