2017 Staff Report

Lessons Learned from Commission-Led CIP Version 5 Reliability Audits

Federal Energy Regulatory Commission October 2017

FEDERAL ENERGY REGULATORY COMMISSION

2017 Staff Report
Lessons Learned from Commission-Led CIP Version 5 Reliability Audits

Prepared by Staff of the

Office of Electric Reliability

Federal Energy Regulatory Commission

Washington, D.C.

October 6, 2017

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

Introduction

The staff of the Division of Reliability Standards and Security in the Office of Electric Reliability, with assistance of staff from the Division of Audits and Accounting in the Office of Enforcement, of the Federal Energy Regulatory Commission (Commission) has completed non-public audits of several registered entities of the Bulk Electric System (BES).[1] The audits evaluated the registered entities' compliance with the applicable mandatory Reliability Standards for the Bulk-Power System Critical Infrastructure Protection (CIP) Reliability Standards (CIP Reliability Standards).[2] Staff from Regional Entities and the North American Electric Reliability Corporation (NERC) participated on the audits, including the on-site portion. The audits were completed during Fiscal Years 2016 and 2017 (FY2016 and FY2017, respectively).

The audits provided audited entities an assessment of their compliance status in the audited areas. Staff found that, for the first series of completed non-public audits, most of the cyber security protection processes and procedures adopted by the audited entities met the mandatory requirements of the CIP Reliability Standards. Staff also found instances of potential compliance infractions. Additionally, staff identified possible areas of improvement in the security posture of audited entities that are not specifically addressed by the CIP Reliability Standards. The audits afforded audited entities opportunities to learn of areas for improvement in their security posture and staff recommended proposals to addresses the matters.

This anonymized summary report informs the regulated community and the public of lessons learned from the audits, including insights into the cyber security and CIP compliance issues encountered by registered entities. This report provides information and recommendations to NERC, Regional Entities, and registered entities that staff believes is useful in their assessments of risk, compliance, and overall cyber security. Moreover, this information may be generally beneficial to the utility-based cyber security community to improve the security of the BES.

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

[2] 18 C.F.R. Part 40 (2017).

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.[3] 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,[4] and subsequently certified NERC.[5]

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.[6] 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.

[3] 16 U.S.C. 824o (2012).

[4] *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).

[5] *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).

[6] *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 FY2016. The audits focused on evaluating compliance with CIP Reliability Standards version 5 (CIP v5) for the period after July 1, 2016.[7] 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).[8]

Audit fieldwork primarily consisted of data requests and reviews, 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 conducted 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 (SMEs); 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 certain assets identified by an entity as High, Medium, or Low Impact; and interviewed compliance program managers, staff, and employees responsible for day-to-day compliance and regulatory oversight activities.

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 sheets, etc., were validated, substantiated, and crosschecked for accuracy as appropriate. For certain CIP Reliability Standard Requirements, sampling was performed to test compliance.

---

[7] *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.

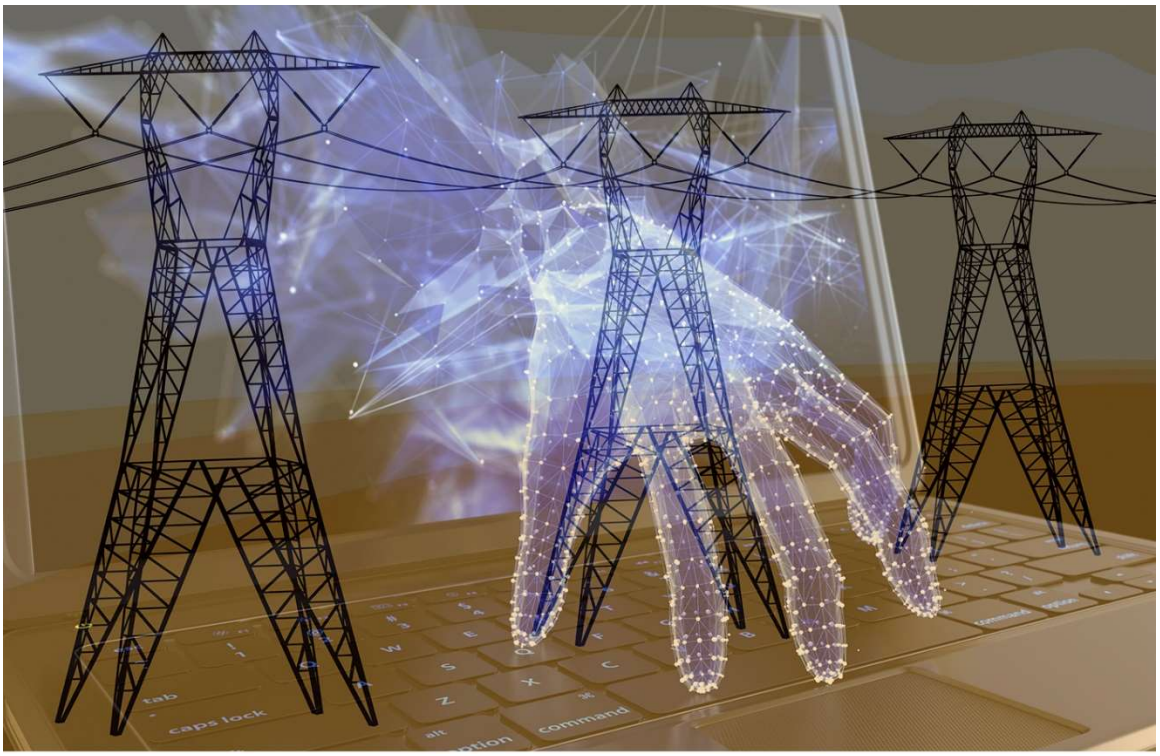
[8] *Revised Reliability Standards for Critical Infrastructure Protection*, 128 FERC ¶ 61,291, *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009), *order on compliance*, 130 FERC ¶ 61,271 (2010); Reliability Standards: CIP-002-3, CIP-003-3, CIP-004-3, CIP-005-3, CIP-006-3, CIP-007-3,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

Overview of Lessons Learned

Staff derived the following lessons learned from the audits it conducted. These lessons are directed toward responsible entities to improve their compliance with the CIP Reliability Standards and their overall cyber security posture.

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, Physical Access Control Systems (PACS), and Electronic Access Control Monitoring Systems (EACMS) or, alternatively, consider the use of automated access rights provisioning.
9. Ensure that access permissions within personnel access tracking systems are clearly mapped to the associated access rights within PACS and EACMS.
10. Ensure that policies and testing procedures for all electronic communications protocols are afforded the same rigor.
11. Perform regular physical inspections of BES Cyber Systems to ensure no unidentified Electronic Access Points (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.



Lessons Learned Discussion

General Practices

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.

Relates To

All CIP Reliability Standards

Entities generally had sufficient security practices that satisfied the CIP Reliability Standards, however documentation on such practices into formal procedures could be improved. Actual practices sometimes included additional steps not included in the formal documented procedures, or differed slightly from the written record on the procedures. Such inconsistencies can have significant impacts on an entity's cyber security program because a lack of complete and accurate documentation of cyber security practices heightens the risk of improper implementation by employees.

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.

Relates To

All CIP Reliability Standards

Audited entities generally performed adequately with regard to having sufficient security controls that satisfied the CIP Reliability Standards, but entities' communications between their various business units could be improved as to these controls. Clear and consistent communication between operational departments and an entity's human resource and information technology departments is imperative to CIP Reliability Standards compliance and the entity's cyber security posture as a whole. For example, poor communication could result in inappropriate delays in revocation of access rights for former employees or transferred employees.

Identifying BES Cyber Systems

3. Consider all owned generation assets, regardless of BES-classification, when evaluating impact ratings to ensure proper classification of BES Cyber Systems.

Relates To
CIP-002-5.1a Requirement R1 Identify BES Cyber Systems

While identification of BES Cyber Systems was generally performed adequately by the audited entities, there was some confusion regarding the generation assets that should be considered when evaluating the rating impact classification of BES Cyber Systems. Reliability Standard CIP-002-5.1a Attachment 1 identifies aggregated thresholds to determine the categorization of a BES Cyber System. For example, Criteria 2.11 requires categorization as Medium Impact of all Control Centers or backup Control Centers, not already categorized as High Impact, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. To determine whether a generation Control Center or back-up Control Center meets the 1500 MW threshold, the MW capacity of both BES generation and non-BES generation are considered. During audit fieldwork, staff found that some entities were only considering BES generation in applying Criteria 2.11, and therefore excluding all "non-BES generation" in their calculations.[9]

For example, a single generator operating with an individual nameplate of 10 MVA would not be included in the BES, and thus not have to categorize its cyber systems. However, a Control Center that controls 150 10-MVA generating resources would have to categorize its cyber systems, some possibly at a Medium Impact rating.[10] Ensuring that all owned generation assets, regardless of BES-classification, are considered in addressing Attachment 1 reduces the risk of improper identification and classification, and insufficient protection, of BES Cyber Systems.

[9] Per the BES Definition, generation resources are included if connected to an Interconnection at a voltage of 100 kV or above and either (a) a gross individual nameplate rating greater than 20 MVA; or, (b) a gross plant/facility aggregate nameplate rating greater than 75 MVA. The BES definition is not used to determine the impact rating of BES Cyber Systems. CIP-002-5.1a Attachment 1 does not define, or differentiate between, the terms "BES Generation," and "Non-BES Generation."

[10] CIP-002-5.1a (Cyber Security - BES Cyber System Categorization), Attachment 1 (Impact Rating Criteria), Criteria 2.11.

4. Identify and categorize cyber systems used for supporting generation, in addition to the cyber systems used to directly control generation.

Relates To
CIP-002-5.1a Requirement R1 Identify BES Cyber Systems

While identification of BES Cyber Systems that were used to directly control generation units was generally performed adequately by the entities, the identification of BES Cyber Systems that are used to control generation "support systems" could be improved.[11] In many cases inadequate documentation of "supporting systems" for BES Cyber Systems may have increased the entity's compliance risk of not correctly identifying all BES Cyber Systems.

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.

Relates To
CIP-002-5.1a Requirement R1 Identify BES Cyber Systems

The coordination between two or more owners of a shared BES facility for compliance with the CIP Reliability Standards could be improved. The identification and categorization of the assets at such shared facilities were not consistently coordinated between the owners. The underlying operating agreements did not clearly delineate the compliance responsibilities of each entity, which heightens the risk of devices being overlooked for required protections.

[11] Generator support systems may include fuel handling, water handling, air handling, exhaust handling, and other systems that are used to support the operations of the unit.

Personnel & Training

6. Conduct a detailed review of the contractor personnel risk assessment processes to ensure sufficiency and to address any gaps.

Relates To
CIP-004-6 Requirement R3 Personnel Risk Assessment Program

Personnel risk assessments (PRA) were generally performed and documented adequately for employees of an entity, but the PRAs for contractors were not consistently performed and documented. These deficiencies largely resulted from entities not evaluating contractors' processes or authorizing different PRA processes for contractors than those the entities used for their own employees. This led to inconsistencies in performance and documentation that heighten the risk of improper management of personnel with access to BES Cyber Systems.

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).

Relates To
CIP-004-6 Requirement R4 Access Management Program

While audited entities generally had sufficient controls to limit electronic access to their PSP (i.e., keypads or badge readers for doors), the controls surrounding the use of physical keys to access PSPs could be improved. Physical keys were used less frequently than electronic access, generally provided access to lower impact facilities, and/or were only used as a secondary means to electronic access. However, the physical keys still provide access to PSPs and should be afforded the same level of control as afforded for electronic access.

8. Enhance procedures, testing, and controls around manual transfer of access rights between personnel accessing tracking systems, Physical Access Control Systems (PACS), and Electronic Access Control Monitoring Systems (EACMS) or, alternatively, consider the use of automated access rights provisioning.

Relates To

CIP-004-6 Requirement R4 Access Management Program

Most entities used either proprietary or customized Enterprise Resource Management systems (e.g., SAP, PeopleSoft, etc.), collectively referred to as Personnel Access Tracking Systems (PATS), to manage the authorization of physical access to their PSPs and electronic access to their BES Cyber Systems. The authorizations would then be promulgated, usually manually, to the corresponding PACS[12] and EACMS,[13] respectively. Staff found that while updates from the PATS to the PACS and EACMS were generally performed adequately, the manual promulgation led to instances of orphan records in the PATS and untimely updates to the PACS and EACMS, heightening the risk of improper access to the entity's PSPs and BES Cyber Systems. The higher risks for access control deficiencies may be due to the manual promulgation of the access rights. Entities should consider a detailed review of their policies and testing procedures for manual promulgation between PATS, PACS, and EACMS, or alternatively consider implementing automated access rights provisioning from the PATS to the PACS and EACMS.

[12] The NERC Glossary defines PACS as Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

[13] The NERC Glossary defines EACMS 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 Intermediate Systems. Examples of EACMS are Active Directory and other types of directory-services servers.

9. Ensure that access permissions within personnel access tracking systems are clearly mapped to the associated access rights within PACS and EACMS.

Relates To

CIP-004-6 Requirement R4 Access Management Program

Access permissions granted by entities within their PATS for employees or contractors may grant multiple types of access (i.e., physical, electronic, or informational). In some cases, these multi-faceted permissions were not clearly mapped to the type of access being granted. Lack of clarity between these permissions and the associated access rights heightens the risk of incorrect access permissions for certain employees or contractors. These risks may be lowered by reviewing the mappings, and clarifying, as appropriate, the PATS permissions within the PACS and EACMS.

Electronic Security Perimeters

10. Ensure that policies and testing procedures for all electronic communications protocols are afforded the same rigor.

Relates To

CIP-005-5 Requirement R1 Electronic Security Perimeter

Most entities use the Internet protocol suite for routable communication. The Internet protocol suite is composed of various protocols encapsulated within Internet Protocol (IP), such as the Transmission Control Protocol (TCP), the Internet Control Message Protocol (ICMP), and the User Datagram Protocol (UDP). While entities generally applied sufficient controls regarding access permissions for most Internet protocol suite communication, controls for all of the Internet protocol suite communication could be improved.

11. Perform regular physical inspections of BES Cyber Systems to ensure no unidentified Electronic Access Points (EAPs) exist.

Relates To

CIP-005-5 Requirement R1 Electronic Security Perimeter

While entities generally used an identified EAP[14] for all External Routable Connectivity (ERC),[15] there were some instances where an identified EAP was not used. These deficiencies usually occurred when a cyber asset within a BES Cyber System was directly connected to an outside network without going through an identified EAP, usually for troubleshooting or maintenance purposes, but the connection was left in place after the troubleshooting or maintenance was complete. Such connections pose a high risk to the security posture of the BES Cyber System.

12. Review all firewall rules and ensure access control lists follow the principle of "least privilege."

Relates To

CIP-005-5 Requirement R1 Electronic Security Perimeter

While entities generally implemented and maintained their firewall rules appropriately, there were some instances where firewall rules will allow traffic from any source or to any destination. This is generally considered to be an insecure access control rule because it employs no aspects of the principle of least privilege. Cybersecurity best practices include minimizing the use of any source or to any destination, as the vulnerability could be used for data exfiltration.

[14] The NERC Glossary defines EAP 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 can be generally or simply considered a "firewall."

[15] The NERC Glossary defines ERC as the ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection. Often the bi-directional routable protocol connection is a protocol from the Internet protocol suite, such as TCP/IP, UDP/IP, or ICMP/IP.

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.

Relates To

CIP-005-5 Requirement R2 Interactive Remote Access Management

Most entities' practices for conducting IRA[16] allow for other network communications to be made by the remote cyber asset conducting the IRA session. Although no current CIP Reliability Standard requirement directly limits other network communications on a remote cyber asset conducting an IRA, limiting all other connections minimizes the overall attack surface of the entity while conducting an IRA and enhances its cyber security posture. Disabling other network access would include: disabling split tunneling if the IRA cyber asset is using a Virtual Private Network to connect to an Intermediate System; disabling dual-homing if the IRA cyber asset has more than one network connection; or disallowing general Internet access.

[16] 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 Electronic Security Perimeter(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.

Physical Security of BES Cyber Systems

14. Enhance processes and controls around the use of manual logs, such as highly visible instructions outlining all of the parts of the requirement with each manual log, to consistently capture all required information.

Relates To

CIP-006-6 Requirement R2 Visitor Control Program

Entities generally maintained complete visitor access control logs of physical access to the PSPs, however certain manual processes could be improved. The use of manual logs in certain instances led to failures to record pieces of information required to be recorded for each visitor (e.g., visitor's name, time of entry, time of exit, etc.). Such deficiencies were sometimes caused by inadequate controls for the use of manual logs. This risk could be lowered if highly visible instructions outlining all of the parts of the requirement were located in or near each manual log.

Systems Security Management

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.

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

While entities generally implemented strong processes for ensuring that only logical network accessible ports that had been determined to be needed were enabled, the documentation of such determinations could be improved. CIP v5 provides a previously unavailable exemption for devices that have no provision for disabling or restricting logical ports. While entities would often document their determination for logical network accessible ports on devices that can disable or restrict logical ports, the entities would often overlook the documentation regarding devices that cannot disable or restrict logical ports. CIP v5 requires entities to document the details of such determination for each cyber asset, even for cyber assets that have no provision for disabling or restricting ports.

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.

Relates To
CIP-007-6 Requirement R3 Malicious Code Prevention

While entities generally had strong processes and procedures to deter, detect, and prevent malicious code at the host level (i.e., within the cyber assets themselves) for all of the Windows-based cyber assets within a BES Cyber System, the processes and procedures around non-Windows based cyber assets could be improved.[17] Historically, non-Windows based cyber assets have had minimal, if any, malicious code designed to disrupt them. The lack of malicious code targeting non-Windows cyber assets combined with lack of options for reliability host based malicious code prevention methods has led entities to rely on network based malicious code prevention. However, malicious code targeting non-Windows cyber assets is on the rise, and there are now reasonable host-based malicious code prevention options available. Entities relying solely on network based malicious code prevention for cyber assets operate at a heightened cyber security risk.

[17] Non-Windows based cyber assets within a BES Cyber System normally are cyber assets running Unix-like operating systems (e.g., Linux, HP-UX, AIX, Solaris).

17. Implement procedures and controls to monitor or limit the number of simultaneously successful logins from different locations.

Relates To

CIP-007-6 Requirement R5 System Access Control

Entities generally had strong procedures and controls for limiting the number of unsuccessful authentication attempts to critical systems and monitoring for unsuccessful authentication attempts through the use of alerts. However, most entities did not have procedures and controls in place to monitor for multiple successful logins to critical systems simultaneously from different locations. Although the CIP Reliability Standards do not specify a limit on the number of simultaneous successful logins a single user can have, and there are legitimate needs for some users to be logged into critical systems simultaneously, it is important to monitor such instances if occurring from different locations to ensure they are authentic.

Configuration Management

18. Implement procedures to detect and investigate unauthorized changes to baseline configurations.

Relates To

CIP-010-2 Requirement R2 Configuration Monitoring

Entities generally had implemented appropriate procedures to monitor for changes to the baseline configurations of their cyber assets, but the procedures for investigating detected unauthorized changes to baseline configurations could be improved. Documented processes for investigating detected unauthorized changes limit the risk that entities will not consistently prevent such unauthorized changes from reoccurring.

Information Protection

19. Ensure that all commercially available enterprise software tools are included in BES Cyber System Information (BSCI) storage evaluation procedures.

Relates To CIP-011-2 Requirement R1 Information Protection

Entities generally had strong procedures in place to identify and protect BCSI stored on most storage platforms (e.g., locked room with drawings containing BCSI information, cyber assets acting as file servers); however, the procedures around BCSI stored in enterprise software tools could be improved. These tools, usually performing functions like logging analysis or configuration management, are commercially available client-server software applications that may be located on an entity's corporate network. Such tools should be afforded the same protection as any other storage platform that contains BCSI.

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."

Relates To CIP-011-2 Requirement R1 Information Protection

While entities generally had sufficient security controls to identify and protect BCSI, most entities' BCSI programs still fell short of the guidance listed in the NERC CIPC[18] document, "Security Guideline for the Electricity Sector: Protecting Sensitive Information."[19] Entities could enhance their documented processes and procedures for identifying BCSI by taking into consideration this NERC CIPC document.

[18] NERC's CIPC coordinates NERC's security initiatives and serves as an expert advisory panel to NERC in the areas of physical security and cybersecurity.

[19] http://www.nerc.com/comm/CIPC/Protecting%20Sensitive%20Information%20Guideline%20Task1/Protecting%20Sensitive%20Information%20Guideline%20(PSIGTF).pdf.

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

Relates To

CIP-011-2 Requirement R1 Information Protection

While entities generally had sufficient security controls to identify and protect BCSI, procedures for labeling, printing, and using external storage to transfer BCSI could be improved. Staff training was often the primary tool for communicating such procedures around BCSI rather than documented formal procedures. This method heightens the risk of improper management of BCSI.