2025

Lessons Learned from Commission-Led CIP Reliability Audits

FEDERAL ENERGY REGULATORY COMMISSION
Office of Electric Reliability
Division of Cyber Security

2025 Lessons Learned from Commission-Led CIP Reliability Audits

A Staff Report

October 20, 2025

FEDERAL ENERGY REGULATORY COMMISSION
Office of Electric Reliability
Division of Cyber Security

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

During Fiscal Year (FY) 2025,[1] staff of the Federal Energy Regulatory Commission (Commission) completed non-public Critical Infrastructure Protection Audits (CIP Audits) of several U.S.-based North American Electric Reliability Corporation (NERC) registered entities.[2] The CIP Audits evaluated registered entities' compliance with the applicable Commission-approved CIP Reliability Standards (Reliability Standards).[3] Staff from NERC and the Regional Registered entities[4] participated in the CIP Audits, including the virtual and on-site portions.

During the CIP Audits, staff found that while most of the cyber security protection processes and procedures adopted by the registered entities met the mandatory requirements of the Reliability Standards, potential noncompliance and security risks remained. Staff also identified practices not required by the Reliability Standards that could improve security, which this report includes, as voluntary cyber security recommendations.[5]

This anonymized summary report informs the regulated community and the public of lessons learned from the FY2025 CIP Audits. This report provides information and recommendations to NERC, Regional Registered entities, and registered entities for use in their assessments of risk and compliance, and to improve overall cyber security. Moreover, this information may be generally beneficial to the utility-based cyber security community to improve the reliability and security of the Bulk-Power System.[6]

[1] The fiscal year is the accounting period for the federal government that begins on October 1st and ends on September 30th. The fiscal year is designated by the calendar year in which it ends; for example, FY2025 began on October 1, 2024, and ended on September 30, 2025.

[2] Section 215 of the Federal Power Act (FPA) gives NERC (as the Commission-certified Electric Reliability Organization (ERO)) the authority to establish and enforce Reliability Standards for users, owners, and operators of the Bulk-Power System. The Reliability Standards are subject to Commission review and approval. 16 U.S.C. § 824o. Registered entities are registered in accordance with the NERC Rules of Procedure. *See* NERC, *Rules of Procedure*, www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

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

[4] NERC, as the ERO, delegates certain authorities, including compliance monitoring and enforcement, to six Regional Registered entities: Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), ReliabilityFirst Corporation (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE), and Western Electricity Coordinating Council (WECC).

[5] The Commission's Office of Energy Infrastructure Security (OEIS) was not involved in these audits. However, 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 Reliability Standards but instead is responsible for the identification and sharing 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.

[6] The Bulk-Power System is defined in section 215 of the FPA as facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. 16 U.S.C. § 824o(a)(1).

CIP RELIABILITY STANDARDS

Section 215 of the FPA provides that the Commission may certify an ERO, the purpose of which is to establish and enforce Reliability Standards, which are subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[7] The Commission established a process to select and certify an ERO,[8] and subsequently certified NERC as that ERO.[9]

The Reliability Standards are designed to mitigate the cyber security and physical security risks to bulk electric system (BES)[10] facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable because of a security incident, would affect the reliable operation of the Bulk-Power System. Pursuant to section 215 of the FPA, on January 28, 2008, the Commission approved an initial set of eight mandatory Reliability Standards pertaining to cyber security.[11] In addition, the Commission directed NERC to develop certain modifications to the Reliability Standards. Since 2008, the Reliability Standards have undergone multiple revisions to address Commission directives and respond to emerging cyber security issues.[12]

The Commission initiated its Reliability Standards audit program for registered entities in FY2016, and the Commission has conducted CIP Audits each year since.

The Reliability Standards may be found on NERC's website. Specific 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-004-7 (Personnel & Training)
4. CIP-006-6 (Physical Security of BES Cyber Systems)
5. CIP-010-4 (Configuration Change Management and Vulnerability Assessments)

[7] 16 U.S.C. § 824o.

[8] *Rules Concerning Certification of the Elec. Reliability Org.; & Procs. for the Establishment, Approval, and Enf't of Elec. Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

[9] *N. Am. Elec. 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] NERC's Commission-approved BES definition is a subset of the Bulk-Power System and one method NERC uses to identify the facilities and elements necessary for the reliable operation and planning of the interconnected Bulk-Power System and the registered entities subject to NERC compliance. Generally included within the BES definition are those elements of the Bulk-Power System that are operated or connected at 100 kV or higher. Other elements or facilities may be added or removed from the BES definition based on application of various inclusions and exclusions that are a part of the definition. *See Revisions to Elec. Reliability Org. Definition of Bulk Elec. Sys. and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012), *order on reh'g*, Order No. 773-A, 143 FERC ¶ 61,053 (2013).

[11] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *denying reh'g and granting clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[12] *See* e.g., *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014); *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, o*rder denying reh'g*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

AUDIT SCOPE AND METHODOLOGY

Audit fieldwork consisted of data requests and reviews, webinars and teleconferences, and virtual and on-site visits. Prior to the virtual and on-site visits, staff issued data requests to gather information on registered entities' CIP activities and operations and held webinars and teleconferences to discuss the audit scope and objectives, data requests and responses, technical and administrative matters, and compliance concerns.

During the virtual and on-site visits, staff:

1. interviewed the registered entities' subject matter experts and observed demonstrations of their staff's operating practices, processes, and procedures;
2. interviewed employees and managers responsible for performing tasks within the audit scope and analyzed documentation to verify compliance with Reliability Standard requirements;
3. conducted several field inspections and observed the functioning of applicable Cyber Assets[13] identified by the registered entity as High, Medium, or Low Impact;[14] and
4. interviewed compliance program managers, staff, and employees responsible for day-to-day compliance.

Applicable Cyber Assets consist of BES Cyber Assets[15] that compose a BES Cyber System,[16] and associated Cyber Assets to that BES Cyber System. Associated Cyber Assets consist of Electronic Access Control or Monitoring Systems (EACMS),[17] Physical Access Control Systems (PACS),[18] and Protected Cyber Assets (PCAs).[19]

The data, information, and evidence provided by the registered entities were evaluated for sufficiency, appropriateness, and validity. Documentation submitted in the form of policies, procedures, e-mails, logs, studies, and data were validated and substantiated as appropriate. For certain CIP Standard requirements, sampling was used to assess compliance.

[13] Cyber Assets refer to programmable electronic devices, including the hardware, software, and data in those devices. NERC, Glossary of Terms Used in NERC Reliability Standards, at 14 (July 10, 2025), www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf(NERC Glossary).

[14] The Reliability Standards require that applicable registered entities categorize their BES Cyber Systems and associated Cyber Assets as High, Medium, or Low Impact according to the criteria found in Reliability Standard CIP-002-5.1a, Attachment 1.

[15] A BES Cyber Asset is 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 BES. 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. *See* NERC Glossary at 75.

[16] A BES Cyber System is one or more BES Cyber Assets logically grouped by an entity to perform one or more reliability tasks for a functional entity. *See* NERC Glossary at 7.

[17] EACMS are "Cyber Assets that perform electronic access control or electronic access monitoring of the [ESP] or BES Cyber Systems. This includes Intermediate Systems." Id. at 12. 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. Reliability Standard CIP-002-5.1a (Cyber Security - BES Cyber System Categorization) at 6.

[18] PACS are Cyber Assets that control, alert, or log access to the Physical Security Perimeter, exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. *See* NERC Glossary at 31.

[19] PCAs are Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter (ESP) that are not part of the highest impact BES Cyber System within the same ESP. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. Put simply, a Protected Cyber Asset is a Cyber Asset that works within a logical network of a BES Cyber Asset but is not itself a BES Cyber Asset. *See* NERC Glossary at 32.

OVERVIEW OF LESSONS LEARNED

The lessons discussed in this report are intended to help registered entities improve their compliance with the Reliability Standards and are presented in numerical order by CIP Standard:

1. **CIP-002-5.1a, R1:** Ensure that BES Asset Identification and Categorization Procedures consider Distributed Energy Resources (DERs) when determining Control Center impact rating.
2. **CIP-003-8, CIP-006-6 and CIP-010-4:** Perform due diligence when relying on third parties to perform compliance duties.
3. **CIP-004-7 and CIP-010-4:** Registered entities should consider the compliance risk when using cloud services.

LESSONS LEARNED DISCUSSION

Control Center Categorization as Required by CIP-002-5.1a, Requirement R1

OVERVIEW

Ensure that BES Asset Identification and Categorization Procedures consider DERs[20] when determining Control Center[21] impact rating.

Reliability Standard CIP-002-5.1a, Requirement R1 requires registered entities to identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. To identify and categorize these systems and assets, registered entities refer to the Reliability Standard's Attachment 1, which defines the criteria for each impact rating. Pursuant to Reliability Standard CIP-002-5.1a, Attachment 1, BES Cyber Systems and associated BES Cyber Assets may be classified as low, medium, or high impact.

Specifically, Attachment 1, criterion 2.11 applies to any Control Center or backup Control Center used to perform GOP functions where, in the preceding 12 calendar months, the aggregate highest rated net Real Power capability of generation resources is equal to or exceeds 1,500 MW within a single interconnection. Criteria 2.11 does not specify that the aggregate generation must be from BES resources. To determine whether a generation Control Center or back-up Control Center meets the 1,500 MW threshold, the MW capacity of both BES generation and non-BES generation are considered.[22]

BACKGROUND

During Commission-led CIP audits conducted during FY 2025, audit staff found that through the entity's identification and categorization process, some registered entities failed to consider DERs and distribution-connected generation in their calculations for aggregate highest net Real Power capability of generation resources, in the proceeding 12 calendar months, when determining the impact rating of a Control Center that was performing GOP functions for those resources.[23]

[20] The Commission defines a DER as "any resource located on the distribution system, any subsystem thereof or behind a customer meter." 18 CFR § 35.28(b)(10). In Order No. 2222, the Commission explained that DERs could include resources located on the distribution system and that are "in front of and behind the customer meter, electric storage resources, intermittent generation, distributed generation, demand response, energy efficiency, thermal storage, and electric vehicles and their supply equipment.'" *See Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators*, Order No. 2222,172 FERC ¶ 61,247, at P 114 (2020), *order on reh'g*, Order No. 2222-A, 174 FERC ¶ 61,197 (2021), *order on reh'g*, Order No. 2222-B, 175 FERC ¶ 61,227 (2021).

[21] A Control Center is one or more facilities hosting operating personnel that monitor and control the BES in real-time to perform the reliability tasks, including the associated data centers, of: (1) a Reliability Coordinator, (2) a Balancing Authority, (3) a Transmission Operator for transmission Facilities at two or more locations, or (4) a Generator Operator (GOP) for generation Facilities at two or more locations. *See* NERC Glossary at 13.

[22] *See* FERC, *See e.g.*, 2017 *Staff Report on Lessons Learned from Commission-Led CIP Version 5 Reliability Audits*, Lesson Learned #3 (Oct. 6, 2017), www.ferc.gov/sites/default/files/2020-05/10-06-17-CIP-audits-report_3.pdf.

[23] *See* NERC, *Rules of Procedure*, App 5A (Organization Registration and Certification Manual) and 5B (Statement of Compliance Registry Criteria) (June 27, 2024), https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

RISK

Audit staff observed that registered entities own and operate a wide mix of generation resources with different net real outputs. This includes larger generation resources with a gross individual nameplate rating greater than 20 MVA or a gross plant/facility aggregate nameplate rating greater than 75 MVA. This mix also includes some registered entities that operate smaller DERs, many below 10 MVA. In some cases, these smaller resources number in the hundreds, adding up to a significant amount of aggregate generation in a single interconnection. For example, audit staff have encountered situations where registered entities have operated over 500 DER resources, with an aggregate net Real Power capability of over 1,700 MVAs in a single interconnection.

Additionally, audit staff observed that some registered entities operated DERs and transmission-connected BES generation resources from the same physical Control Center, using the same personnel. These conditions fail to meet the physical segmentation principles outlined in CIP-002-5.1a, which were also addressed in last year's 2024 Lessons Learned from Commission-led CIP Reliability Audits.[24]

In situations where the entity operates both BES and non-BES generation from the same Control Center, the net Real Power capability of all combined generation should be accounted for when applying CIP-002-5.1a Attachment 1, Section 2.11 to determine the impact level of the Control Center.

Identification and categorization are the foundation of the Reliability Standards. Failure to properly categorize BES cyber systems with the appropriate impact rating means that an entity may not apply the required controls consistent with the risk. These missing controls may negatively impact the reliable operation of the BES.

MITIGATION

When identifying their Control Centers, registered entities should assess and document generation resources holistically, including DERs. When these resources are being operated from the same Control Center, and aggregated capacity exceeds 1,500 MW in a single interconnection, the Control Center must be categorized as Medium Impact under Attachment 1, Section 2.11.

ADDITIONAL GUIDANCE

FERC

Order No. 2222
www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

NOTE: See PP 114 and page 93.

NIST

SP 800-53 rev. 5: Security and Privacy Controls for Information Systems and Organizations
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NOTE: See section RA-9 and page 247. Criticality Analysis: Identify critical system components and functions by performing a criticality analysis

[24] CIP-002-5.1a, R1: Ensure logically segmented Control Centers at a single site location are evaluated as a single Control Center in BES Asset identification and categorization procedures. *See* FERC Staff, *2024 Lessons Learned from Commission-Led CIP Reliability Audits*, at 7-8 (2024), www.ferc.gov/sites/default/files/2024-08/24_Lessons Learned_0826.pdf.

CISA

Foundation for OT Cybersecurity: Asset Inventory Guidance for Owners and Operator
www.cisa.gov/sites/default/files/2025-08/joint-guide-foundations-for-OT-cybersecurity-asset-inventory-guidance_508c.pdf

NOTE: See section Maintenance and Reliability and page 12. Analyze OT spare parts inventory to determine whether the stockpile of spare OT components sufficiently covers the critical assets identified in the inventory to ensure operational reliability.

Use of Third Parties to Perform Reliability Standards Compliance Duties CIP-003-8, CIP-006-6, and CIP-010-4

OVERVIEW

Perform due diligence when relying on third parties to perform compliance duties.

Registered entities are ultimately responsible for compliance with the applicable Reliability Standards, even when using third parties for their compliance obligations. Thus, if registered entities use third parties to perform a function that could impact compliance, they must ensure their third parties comply with the Reliability Standards. Third parties may include contractors, sub-contractors, vendors, and consultants, which may be located on or off premise. While the NERC ERO Registration Procedure allows registered entities to "delegate the performance of a task to another entity, including a non-registered party, using a third-party agreement," it also makes clear that "the registered entity remains solely responsible for compliance and is accountable for violations even with respect to tasks performed by the non-registered third-party on its behalf."[25] Further, registered entities are required to provide evidence of compliance to audit staff, including those tasks performed by third parties for CIP Standard compliance. For example, registered entities should have written evidence available to demonstrate third-party completion of assigned tasks and adherence to the NERC Rules of Procedure (ROP) for Data Access.[26]

BACKGROUND

Registered entities often rely on third parties to perform services that support registered entities in fulfilling their Reliability Standards compliance duties. When engaging third parties, registered entities should conduct appropriate oversight of assigned activities and assure that associated risks are properly and timely mitigated. The Commission explained in Order No. 706:[27]

> [w]hile such [outsourced] providers are not registered entities subject to the Reliability Standards, they must perform the services and operate the applications in a manner consistent with the Reliability Standards. . . the Responsible Entity should be charged with incorporating contractual terms and conditions into agreements with third-party service providers that obligate the providers to comply with the requirements of the Reliability Standards.
>
> Further, it is incumbent upon a responsible entity to conduct vigorous oversight of the activities and procedures followed by the vendors they employ.

[25] NERC, *ERO Enterprise Registration Procedure*, at 7-8 (Feb. 3, 2022), www.nerc.com/pa/comp/RegistrationReferenceDocsDL/ERO%20Enterprise%20Registration%20Procedure.pdf.

[26] *See* NERC, *Rules of Procedure*, sec. 401.3 Data Access ("All Bulk Power System owners, operators, and users shall provide to NERC or the Compliance Enforcement Authority (CEA) such Documents, data, and information as is necessary to monitor and enforce compliance with the Reliability Standards."). *See also id.*, sec. 403.9 ("Information Submittal — All Bulk Power System owners, operators, and users responsible for complying with Reliability Standards within the Regional Entity shall submit timely and accurate Documents, data, and information when requested by the Regional Entity or NERC.").

[27] Order No. 706, 122 FERC ¶ 61,040, at 52 and 53.

Audit staff found that while registered entities generally conducted due diligence and proper oversight of the compliance tasks performed by their third parties, in some cases registered entities did not consistently conduct proper oversight, retain evidence, or have sufficient oversight controls in place that led to the entity being out of compliance.

RISKS

Audit staff observed several instances where registered entities did not perform due diligence when relying on third parties. For example, one audited entity contracted most of its Reliability Standards compliance program to a third-party, but the entity did not perform oversight to ensure that the third-party fulfilled those responsibilities. The following examples illustrate additional instances of staff concerns regarding third party oversight:

1. **CIP-003-8 R2, Attachment 1, Section 3**

   Pursuant to Reliability Standard CIP-003-8, Requirement R2, registered entities with assets containing Low Impact BES Cyber Systems must implement one or more documented cyber security plan(s). An entity's plans must include the elements specified in Attachment 1 of Reliability Standard CIP-003-8. Section 3 of Attachment 1 specifies necessary controls pertaining to Electronic Access Controls.[28]

   Staff observed that one audited entity did not perform oversight of a task it contracted to a third-party, and the third-party did not complete the task. Specifically, the registered entity contracted with the third-party to ensure that all firewall rules were up to date and necessary. The third-party, however, did not complete the task, which left unnecessary inbound and outbound electronic access within the entity's firewall, inconsistent with Reliability Standard CIP-003-8, Attachment 1, section 3. Additionally, the registered entity lacked oversight controls, which required a delayed, after-the-fact follow-up with the third party to ensure that it completed the task.

2. **CIP-006-6 R3.1**

   Reliability Standard CIP-006-6, Requirement R3 requires registered entities with assets containing applicable High and Medium Impact PACS to implement one or more documented PACS maintenance and testing program(s). Further, registered entities must perform maintenance and testing of each PACS and locally mounted hardware or devices at the Physical Security Perimeter[29] at least once every 24 calendar months.[30]

   One entity relied on a vendor to conduct installation, testing, and maintenance of a third-party cloud-based PACS. Once installation was completed, the entity relied on the vendor to conduct the recurring, 24-month testing as required by the Standard. The vendor, however, failed to conduct the testing on the PACS in the required timeframe. The entity did not have proper oversight controls to ensure that the vendor met the testing requirements or timely learn of the third party's failure to do so.

3. **CIP-010-4 R3**

   Reliability Standard CIP-010-4, Requirement R3 requires registered entities with assets containing High and Medium Impact Cyber Assets to implement a vulnerability assessment program to protect BES Cyber Systems against vulnerabilities that, if exploited, could lead to the compromise of the BES.

[28] CIP-003-8 R2, Attachment 1 (Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems), Section 3.

[29] 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. *See* NERC Glossary at 31.

[30] *See* Reliability Standard CIP-006-6, Table R3 (Physical Access Control System Maintenance and Testing Program), Part 3.1.

A registered entity performing a vulnerability assessment retained a third party to conduct specific tasks, namely vulnerability scanning, reviewing scanned results, and prioritizing mitigation plans. The registered entity did not participate in the analysis and assessment of the scan results or the prioritization of the mitigation plan. The entity should have conducted regular review meetings and joint prioritization sessions, to ensure that vulnerability mitigation plans aligned with organization risk tolerance and operational priorities.

Using third parties to perform Reliability Standards compliance tasks has benefits and risks that registered entities should consider before retaining the third-party vendor. Moreover, a registered entity should continuously monitor and manage the third party through due diligence and oversight. Third parties can provide financial and technological benefits for registered entities in the continuously evolving technology landscape. However, third parties can increase risks due to a lack of security controls or unsecure infrastructure that the entity may not directly manage, thus increasing the likelihood of vulnerabilities to the environment. Without entity oversight of the third-party's assigned tasks, there is a higher chance of undetected noncompliance, which could lead to security breaches, data loss, or regulatory violations. Additionally, if an issue arises from unverified third-party performance, it could lead to broader organizational challenges, underscoring the value of taking thoughtful, proactive steps to manage risk.

MITIGATION

Registered entities should consider the following mitigation activities when delegating compliance responsibilities to third parties to ensure the entity's compliance with the Reliability Standards.

1. Registered entities should document and track the security and compliance risks posed by outsourcing functions and processes to a third-party in their supply chain risk management plan.

2. Registered entities should implement compensating controls to reduce the compliance and security risk of using third parties. Examples of compensating controls include:

   2.1. Contractual agreements (Service Level Agreements, Memorandum of Understandings, etc.)

   2.2. Internal controls that provide oversight through monitoring and alerting of third-party actions.

   2.3. Ensure third-party staff, infrastructure, and data, are located within the continental United States.

ADDITIONAL GUIDANCE

NERC
Security Guidelines – Vendor Risk Management Lifecycle
www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf

NERC
Guideline for the Electricity Sector Supply Chain Procurement Language
www.nerc.com/comm/RSTC_Reliability_Guidelines/Procurement_Language_FINAL.pdf

DOE

Cybersecurity Procurement Language for Energy Delivery Systems

www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014

NIST

SP 800-53 rev. 5: Security and Privacy Controls for Information Systems and Organizations

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NOTE: See section PS-3 Personnel screening on page 223. Screen individuals prior to authorizing access to the systems and rescreen individuals in accordance with organization defined conditions.

Compliance Risk of Using Cloud Services CIP-004-7 and CIP-010-4

OVERVIEW

Registered entities should consider the compliance risk when using cloud services.

Registered entities failed to demonstrate compliance with Reliability Standards when using cloud services to perform the function of an associated Cyber Asset, such as an EACMS and PACS.[31] When using cloud service providers, each registered entity is required to implement processes, procedures, and controls for all BES Cyber Systems, associated Cyber Assets, and BES Cyber System Information per each applicable CIP requirement.

BACKGROUND

Cloud services are increasing in popularity across industries, including the energy sector. The benefits of utilizing cloud services include cost savings, availability and scalability, business continuity (e.g., back-up and disaster recovery), security posture of systems (i.e., physical and cyber), efficiency, and accessibility.

As a general matter, the initial CIP Standards were developed prior to the advent of cloud services and registered entities housed their cyber assets and cyber systems on premises. The currently effective CIP Standards do not mention, and simply do not contemplate, cloud services. As a result, registered entities seeking to utilize cloud services do not have a clear path to implement processes, procedures, and controls for associated Cyber Assets to BES Cyber Systems and to demonstrate CIP compliance.[32] NERC has initiated a standards development project to update the CIP Standards to support the use of cloud services while also addressing related security risks.[33] Until NERC completes and the Commission approves the project to update the CIP Standards, registered entities seeking to use cloud services will continue to have challenges demonstrating CIP compliance.

For example, implementing Reliability Standard CIP-004-7 (Cyber Security – Personnel & Training) in a cloud environment can present unique compliance challenges, particularly regarding personnel oversight. One major challenge is conducting and demonstrating personnel risk assessments, as required by Requirement R3, especially for individuals employed by a cloud service provider (CSP). Since these individuals are not directly managed by the organization, registered entities may be unable to confirm identity verification and background checks for those CSP employees. Similarly, registered entities may find it difficult to maintain control regarding security awareness training, especially if third-party contractors (i.e., CSP personnel) are involved.

As another example, Reliability Standard CIP-010-4 (Cyber Security — Configuration Change Management and Vulnerability Assessments) requires the development, maintenance, and documentation of a baseline configuration that includes the operating system, applications, ports, patches, and custom software. For proprietary reasons, CSPs often abstract hardware and system-level configurations making it difficult for organizations to define or maintain a baseline. In addition, in most CSP environments, registered entities may find it extremely difficult to

[31] BES Cyber Systems have "associated Cyber Assets," which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (EACMS and PACS). *See* Reliability Standard CIP-002-5.1a at 6.

[32] *See* NERC Whitepaper, *Virtualization and Future Technologies*, at iv and 9-10 (April 2019).

[33] *See* NERC Project 2023-09 Risk Management for Third-Party Cloud Services.

verify the integrity and source of a given software as set forth in CIP-010-4, Requirement R1.6.[34] It is also unlikely that a CSP would allow an entity to perform an active vulnerability assessment within a cloud environment as required pursuant to Requirement R3.1.[35]

While many registered entities are aware of the above compliance concerns, audit staff have observed circumstances in which entities adopted the use of cloud services without the ability to fully demonstrate CIP compliance. First, registered entities that utilize cloud services for their low impact BES Cyber Systems (which is viable due to the lesser set of CIP compliance obligations) may have their BES Cyber Systems redesignated as medium impact due to a change in circumstances such as the addition of new assets. With that redesignation, entities have found themselves in a predicament that they can no longer fully demonstrate CIP Standard compliance for their cloud operations. Second, certain vendors have made claims that their cloud services are CIP compliant. In fact, the vendors' services were able to perform the PACs function of restricting access to the Physical Security Perimeter as required by CIP-006-6 but were unable to demonstrate compliance with other CIP Standards notably CIP-004-7, CIP-007-6 and CIP-010-4. This confusion has resulted in findings of non-compliance during CIP Standard audits.

Audit staff found that while registered entities generally implemented policies, procedures, and controls when using cloud services for BES Cyber Security Information (BCSI),[36] registered entities failed to demonstrate compliance for cloud services that provided the function of associated Cyber Assets to BES Cyber Systems.

RISK

During FY 2025, audit staff identified two instances where registered entities used cloud services for EACMS and PACS. In the first instance, audit staff identified an entity using a CSP Software as a Service (SaaS) service model to maintain and operate its PACS. Audit staff found that the entity did not have a documented agreement to include roles, responsibilities, security controls and compliance requirements. In this case, the entity was unable to demonstrate compliance with requirements of the applicable Reliability Standards CIP-004-7 and CIP-010-4.

In the second instance, audit staff observed an entity using a CSP for multifactor authentication services in support of EACMS and remote desktop protocol access into devices within the electronic security perimeter. Audit staff found that this second entity also did not have a documented agreement to include roles, responsibilities, security controls and compliance requirements. The entity was unable to demonstrate compliance with Reliability Standards CIP-004-7 and CIP-010-4.

As discussed above, while cloud services offer some clear advantages to registered entities, currently enforceable Reliability Standards do not address deployment of EACMS or PACS in the cloud. In addition, before initiating the use of cloud services, an entity should consider associated security concerns and vulnerabilities such as different attack

[34] Requirement R1.6 requires that "[p]rior to a change that deviates from the existing baseline configuration an entity must verify associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:
1.6.1. Verify the identity of the software source; and verify
1.6.2. Verify the integrity of the software obtained from the software source."

[35] Requirement R3.1 requires that "[a]t least once every 15 calendar months, conduct a paper or active vulnerability assessment."

[36] BCSI is "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." *See* NERC Glossary at 7.

surface, misconfigurations and the shared physical and logical controls between the Registered Entity and the CSP.

For registered entities that choose to use cloud services, the CSPs, not registered entities, will have most, if not all, control of hardware, software and data hosted in the cloud, including but not limited to operations, maintenance, security, and physical access. For this reason and because of the issues described above, it is currently unlikely that entities can provide the measures needed to demonstrate compliance with the relevant Reliability Standards.

MITIGATION

In general, it is a strong cyber security practice to consider both benefits and risks when deciding whether to use cloud services. Registered entities should understand the current limitations of the CIP standards have when operating high and medium impact BES cyber systems in the cloud. Registered entities with low impact BES cyber systems can use cloud services but should understand that a change in designation to medium impact BES cyber systems will have commensurate CIP compliance consequences. Registered entities should specifically consider the following areas.

- **Newly registered entities:** should review their BES Cyber System(s) for awareness of any potential component of its systems that use any cloud services.

- **Entities that operate low impact BES Cyber Systems:** that currently use cloud services should verify their BES cyber system impact rating has not changed, and if so, take the appropriate steps to mitigate the compliance risk associated with using the cloud.

- **Entities that operate high and medium impact BES Cyber Systems:** should continue to review their software, systems, and services to verify that their BES Cyber Systems do not contain components in the cloud.

ADDITIONAL GUIDANCE

NIST
SP 800-53 rev. 5: Security and Privacy Controls for Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NOTE: See section CA-3 Information Exchange on page 86-87. Approve and manage the exchange of information between the system and other systems using interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements.

NERC
Implementation Guidance: Usage of Cloud Solutions for BES Cyber System Information (BCSI) (June 2023)
www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-004-7%20R6%20and%20CIP-011-3%20R1%20-%20Cloud%20Solutions%20for%20BCSI%20(RSTC).pdf

NERC
Cyber Security - Risk Management for Third-Party Cloud Services
https://www.nerc.com/pa/Stand/Pages/Project-2023-09-Risk-Management-for-Third-Party-Cloud-Services.aspx

NIST
SP 800-146 Cloud Computing Synopsis and Recommendations
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

NOTE: See section 3. Typical Commercial Terms of Service on page 3-1. Provider promises, including explict statements regarding limitations, are codified in their service agreements.

NIST
SP 800-210: General Access Control Guidance for Cloud Systems
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf

NOTE: section 3.5 Recommendation for IaaS Access Control on page 9-10. A service level See agreement should be designed to include appropriate control to secure external interoperations.

Cloud Security Alliance
7 Essential SaaS Security Best Practices
cloudsecurityalliance.org/blog/2024/09/12/7-essential-saas-security-best-practices#

NOTE: See 7. Map SaaS to Your Compliance Programs. The people responsible for compliance should know where SaaS apps store data that's relevant to regulations and industry compliance framework.

UK National Cyber Security Centre
Using Software as a Service (SaaS) securely
www.ncsc.gov.uk/collection/cloud/using-cloud-services-securely/using-saas-securely

NOTE: See Understand the application and its purpose. Identifying who will be using the application, the sensitivity of the data it may handle, and the regulatory requirements it may need to comply with.

2017-2024 PREVIOUS LESSONS LEARNED RECOMMENDATIONS

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
All	All	Enhance internal compliance and controls programs to include control documentation processes and associated procedures pertaining to compliance with the Reliability Standards.	2021
All	All	Conduct a thorough review of 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.	2017
All	All	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.	2017
All	All	Consider the use of secure administrative hosts to perform administrative tasks when accessing either EACMS or PACS.	2018
CIP-002-5.1a	Requirement R1	Assess the utility of additional security controls beyond those that are required after identifying and categorizing all BES Cyber Systems and their associated BES Cyber Assets.	2024
CIP-002-5.1a	Requirement R1	Modify BES Asset identification and categorization procedures to consider logically segmented Control Centers as one single Control Center.	2024
CIP-002-5.1a	Requirement R1	Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets.	2023

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-002-5.1a	Requirement R1	Enhance policies and procedures to include evaluation of Cyber Asset misuse and degradation during asset categorization.	2021
CIP-002-5.1a	Requirement R1	Ensure that all BES Cyber Assets are properly identified.	2020
CIP-002-5.1a	Requirement R1 Attachment 1 Criterion 2.5	Ensure that all substation BES Cyber Systems are properly categorized as high, medium, or low impact.	2020
CIP-002-5.1a	Requirements R1 Attachment 1 Criterion 2.8	Consider all generation assets, regardless of ownership, when categorizing BES Cyber Systems associated with transmission facilities.	2019
CIP-002-5.1a	Requirement R1	Consider all owned generation assets, regardless of BES-classification, when evaluating impact ratings to ensure proper classification of BES Cyber Systems.	2017
CIP-002-5.1a	Requirement R1	Identify and categorize cyber systems used for supporting generation, in addition to the cyber systems used to directly control generation.	2017
CIP-002-5.1a	Requirement R1	Ensure that all shared facility categorizations are coordinated between the owners of the shared facility through clearly defined and documented responsibilities for Reliability Standards compliance.	2017

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-003-8 CIP-007-6 CIP-008-6	Requirement R2, Section 4 Requirement R4 Requirement R4	Ensure reportable Cyber Security Incidents and attempts to compromise that were identified as Cyber Security Incidents are reported to Electricity Information Sharing and Analysis Center (E-ISAC) and Cybersecurity and Infrastructure Security Agency (CISA).	2023
CIP-003-8	Requirement R2	Re-evaluate policies, procedures, and controls for Low-impact Cyber Systems and associated Cyber Assets.	2022
CIP-003-8	Requirement R2, Attachment 1, Section 5.2.1	Properly document and implement policies, procedures, and controls for low impact TCAs.	2021
CIP-004-6	Requirement R4	Implement a defined workflow to enhance processes for the verification of electronic access, unescorted physical access, and access to BES Cyber System Information (BCSI).	2021
CIP-004-6	Requirement R4.1.3	Base access to BCSI on "need to know."	2021
CIP-004-6	Requirements R4 and R5	Ensure that access to BES Cyber System Information (BCSI) is properly authorized and revoked.	2020
CIP-004-6	Requirement R2	Ensure that all employees and third-party contractors complete the required training and that the training records are properly maintained.	2019
CIP-004-6	Requirement R4	Verify employees' recurring authorizations for using removable media.	2019

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-004-6	Table R1 Security Awareness Program	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.	2018
CIP-004-6	Requirement R3	Conduct a detailed review of contractor personnel risk assessment processes to ensure sufficiency and to address any gaps.	2017
CIP-004-6	Requirement R4	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	2017
CIP-004-6	Requirement R4	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.	2017
CIP-004-6	Requirement R4	Ensure that access permissions within personnel access tracking systems are clearly mapped to the associated access rights within PACS and EACMS.	2017
CIP-005-7	Requirement R1.3	Restrict all inbound and outbound access permissions, including the reason for granting access and denying all other access by default.	2023
CIP-005-5	Requirement R1	Review all firewalls to ensure there are no obsolete or overly permissive firewall access control rules in use.	2019

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-005-5	Requirement R2	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.	2018
CIP-005-5	Requirement R1	Ensure that policies and testing procedures for all electronic communications protocols are afforded the same rigor.	2017
CIP-005-5	Requirement R1	Perform regular physical inspections of BES Cyber Systems to ensure no unidentified EAPs exist.	2017
CIP-005-5	Requirement R1	Review all firewall rules and ensure access control lists follow the principle of “least privilege.”	2017
CIP-005-5	Requirement R2	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.	2017
CIP-005-5 and CIP-007-6	Requirement R1 and R5	Consider implementing valid Security Certificates within the boundaries of BES Cyber Systems with encryption sufficiently strong to ensure proper authentication of internal connections.	2018
CIP-006-6	Requirement R1	Consider having a dedicated visitor log at each physical security perimeter access point.	2020
CIP-006-6	Requirement R1	Consider locking BES Cyber Systems’ server racks where possible.	2020

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-006-6	Requirement R1	Inspect all physical security perimeters periodically to ensure that no unidentified physical access points exist.	2020
CIP-006-6	Requirement R1	Limit access to employee's personal identification numbers used for accessing physical security perimeters using a least-privilege approach.	2019
CIP-006-6	Requirement R2	Enhance processes and controls around the use of manual logs, such as using highly visible instructions outlining all the parts of the requirement with each manual log, to consistently capture all required information.	2017
CIP-007-6	Requirement R1	Ensure physical and logical port protection controls for Cyber Assets.	2021
CIP-007-6 & CIP-010-4	Requirement R2.3 & Requirement 3.4	Address risks posed by BES Cyber Assets that have reached the manufacturer-determined end of life/service and are no longer supported by vendors.	2022
CIP-007-6	Requirement R3	Deploy a comprehensive malicious code prevention program for all Cyber Assets within a BES Cyber System.	2022
CIP-007-6	Requirement R5	Review the system access control program periodically to ensure processes and procedures are implemented as documented.	2021
CIP-007-6	Requirement R2	Review security patch management processes periodically and ensure that they are implemented properly.	2020

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-007-6	Requirement R5	Consider consolidating and centralizing password change procedures and documentation.	2020
CIP-007-6	Requirement R1	Ensure that all ephemeral port ranges are within the Internet Assigned Numbers Authority (IANA) recommended ranges.	2019
CIP-007-6	Requirement R1	Consider Internet Control Message Protocol (ICMP) as a logical access port for all the BES Cyber Assets.	2018
CIP-007-6	Requirement R2	Consider incorporating file verification methods, such as hashing, during manual patching processes and procedures, where appropriate.	2018
CIP-007-6	Requirement R1	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.	2017
CIP-007-6	Requirement R3	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.	2017
CIP-007-6	Requirement R5	Implement procedures and controls to monitor or limit the number of simultaneously successful logins to multiple different systems.	2017
CIP-007-6 and CIP-010-2	Requirement R2 and R1	Consider replacing or upgrading “End-of-Life” system components of an applicable Cyber Asset.	2018

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-008-5	Incident Reporting and Response Planning	Enhance documented processes and procedures for incident response to consider the NIST SP 800-61, "Computer Security Incident Handling Guide."	2018
CIP-009-2	Requirement R2	Enhance recovery and testing plans to include a sample of any offsite backup images in the representative sample of data used to test the restoration of BES Cyber Systems.	2021
CIP-009-6	Requirement R1	Ensure that backup and recovery procedures are updated in a timely manner.	2020
CIP-010-4	Requirement R1	Document baselines for intentionally-installed, commercially available software on each Cyber Asset.	2024
CIP-010-2	Requirement R3	Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.	2020
CIP-010-2	Requirement R4	Clearly mark TCAs and Removable Media.	2019
CIP-010-2	Requirement R3	Consider the remote configuration of applicable Cyber Assets via a TCP/IP-to-RS232 Bridge during vulnerability assessments.	2018
CIP-010-2	Table R2 Configuration Monitoring	Consider using automated mechanisms that enforce asset inventory updates during configuration management.	2018
CIP-010-2	Requirement R2	Implement procedures to detect and investigate unauthorized changes to baseline configurations.	2017

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-010-3	Requirement R1	Review configuration change management processes periodically and ensure that they are implemented properly.	2021
CIP-010-3	Requirement R1.5	Enhance configuration change management procedures and controls to document and account for differences between test and production environments.	2021
CIP-010-3	Requirement R3	Improve vulnerability assessments to include credential-based scans of Cyber Assets.	2021
CIP-010-3	Requirement R4	Properly document and implement policies, procedures, and controls for medium and high impact TCAs.	2021
CIP-010-4	Requirement R3	Implement comprehensive vulnerability assessment processes for applicable Cyber Assets.	2022
CIP-010-4	Requirement R4	Review and validate controls used to mitigate software vulnerabilities and malicious code on Transient Cyber Assets (TCAs) managed by a third-party. TCAs are generally portable electronic devices used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	2022
CIP-011-2	Requirement R1	Identify, monitor, and protect BES Cyber System Information (BCSI) to mitigate the risks posed by unauthorized access to BCSI.	2024
CIP-011-2	Requirement R1.2	Enhance policies and procedures to include BCSI spillage investigation and response.	2021
CIP-011-2	Requirement R1.1.2	Enhance policies, procedures, and controls to properly track, document and monitor BCSI storage locations.	2021

CIP Standard(s)	CIP Requirement(s)	Lesson Learned	Year of Issuance
CIP-011-2	Requirement R2	Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.	2020
CIP-011-2	Requirement R1	Ensure that all commercially available enterprise software tools are included in BSCI storage evaluation procedures.	2017
CIP-011-2	Requirement R1	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."	2017
CIP-011-2	Requirement R1	Document all procedures for the proper handling of BCSI.	2017
CIP-011-2	Requirement R1.2	Ensure that all the security controls implemented by third parties are evaluated regularly and implement additional controls where needed when using a third-party to manage BES Cyber System Information (BCSI).	2020
CIP-012-1	Requirement R1	Identify all Control Center to Control Center communications that include Real-time Assessment or Real-time Monitoring (RTA/RTM) data and apply security controls to reduce the risk of unauthorized disclosure and unauthorized modification of that data.	2024
CIP-013-1	Requirement R1	Enhance supply chain risk management programs to include evaluating the supply chain risks of existing vendors and develop a plan to respond to the risks that are identified.	2023

FEDERAL ENERGY REGULATORY COMMISSION
Office of Electric Reliability
Division of Cyber Security

FERC.GOV