

2026

Lessons Learned from Commission-Led CIP Reliability Audits



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

2026

Lessons Learned from Commission-Led CIP Reliability Audits

A Staff Report
October 13, 2026



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

- I. Introduction 1
- II. CIP Reliability Standards 4
- III. 2026 Lessons Learned 5
 - A. Timely Registration and CIP Compliance for Generation Resources 6
 - B. Identify and Categorize All BES Cyber Systems Used for Generation Operation 9
 - C. Access to BES Cyber Systems and BES Cyber System Information Facilitated by SI Tools 11

INTRODUCTION

The Federal Energy Regulatory Commission (FERC or Commission) initiated its Critical Infrastructure Protection (CIP) audits program for registered entities in fiscal year (FY) 2016.¹ During FY 2026, FERC staff completed non-public 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 FERC-approved CIP Reliability Standards pertaining to cybersecurity.³ Staff from NERC and its Regional Entities participated in the CIP audits, including the virtual and on-site portions.⁴

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

This anonymized summary report informs the regulated community and the public of lessons learned from the FY 2026 CIP audits.⁶ This report provides information and recommendations to NERC, Regional Entities, and registered entities for use in their assessments of risk and compliance, and to improve overall cybersecurity. Moreover, this information may be generally beneficial to the utility-based cybersecurity community to improve the reliability and security of the Bulk-Power System.⁷

This report highlights three key lessons learned from the FY 2026 CIP Audits:

1. Audit staff found that several Generator Owners did not timely register new generation resources with NERC or promptly identify and categorize associated BES Cyber Systems under Reliability Standard CIP-002-5.1a. Misinterpretations of the Commercial Operation Date (COD) contributed to delays in implementing mandatory cybersecurity requirements, increasing the risk of inadequate or missing protections.

-
- 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, FY2026 began on October 1, 2025, and ended on September 30, 2026.
 - 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 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 entities: Midwest Reliability Organization, Northeast Power Coordinating Council, ReliabilityFirst, SERC Reliability Corporation, Texas Reliability Entity, and Western Electricity Coordinating Council.
 - 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 Previous lessons learned reports are located on the Lessons Learned tab on the *Commission's Staff Reports and Papers* webpage, found here: www.ferc.gov/staff-reports-and-papers. Additionally, a summary of all previous lessons can be found at the same location.
 - 7 Section 215 of the FPA defines the Bulk-Power System as: "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation 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).

2. Audit staff identified instances in which entities did not adequately account for monitoring and control functions performed by affiliates and third-party contractors when identifying and categorizing BES Cyber Systems. In both scenarios, aggregated control capabilities presented greater risk than the capabilities of individual Generator Operators. As a result, potentially medium-impact BES Cyber Systems were treated as low-impact systems and subject to controls that were not commensurate with their risk.
3. Audit staff observed increasing use of super intelligence (SI) tools,⁸ including chatbots, personal assistants, and automated analytical systems, within CIP-networked environments.⁹ Although these tools can improve operational efficiency, their evolving capabilities may introduce access control risks when access is not properly authorized, verified and monitored. Entities must ensure that SI-facilitated access is appropriately controlled, regularly reviewed, and addressed within existing risk management frameworks.

Together, these lessons underscore the need for timely compliance, comprehensive identification and accurate categorization of BES Cyber Systems, and access controls commensurate with risk. These practices must account for functions performed by affiliates and contractors as well as access facilitated by emerging SI technologies. The lessons reinforce the foundational role of the CIP Reliability Standards in safeguarding the reliable and secure operation of the Bulk-Power System.

8 SI tools are software systems that utilize super intelligence to perform tasks traditionally requiring human intelligence. Examples include ChatGPT, Google Gemini, and Microsoft 365 Copilot.

9 In Order 907, the Commission clarified that the “CIP-networked environment” includes the portion of an entity’s network that supports in-scope CIP assets. This environment includes networks inside the Electronic Security Perimeter (ESP) as well as associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). See *Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring*, Order No. 907, 90 FR 28889 (July 2, 2025), 191 FERC ¶ 61,224 at P 43 (2025), *order on reh’g*, Order No. 709-A, 192 FERC ¶ 61,171 (2025).

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' cybersecurity activities and operations and held videoconferences 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 CIP Reliability Standard requirements;
3. conducted field inspections and observed the functioning of applicable cyber assets; and
4. interviewed compliance program managers, staff, and employees responsible for day-to-day compliance.

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 Reliability Standard requirements, sampling was used to assess compliance.

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.¹⁰ Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.¹¹ The Commission established a process to select and certify an ERO¹² and subsequently certified NERC as that ERO.¹³

The CIP Reliability Standards, one of fourteen families of Reliability Standards, are designed to mitigate the cybersecurity and physical security risks to bulk electric system (BES) 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.¹⁴

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.¹⁵ In addition, the Commission directed NERC to develop certain modifications to the Reliability Standards. Since 2008, the CIP Reliability Standards have undergone multiple revisions to address Commission directives and respond to emerging cybersecurity issues.

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-004-7 \(Personnel & Training\)](#)

10 Reliability Standards means requirements “to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the bulk-power system....” *Id.* § 824o(a)(3).

11 *Id.* § 824o(d).

12 *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).

13 *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 ¶ 61,030, *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).

14 NERC’s Commission-approved BES definition is a subset of the Bulk-Power System and is used 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 & clarification*, Order No. 773-A, 143 FERC ¶ 61,053 (2013).

15 *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).

2026 LESSONS LEARNED

The lessons below are intended to help registered entities improve their compliance with the CIP Reliability Standards:

1. CIP-002-5.1a, R1: Ensure that all generation resources that are synchronized to the BES and generating power greater than the applicable threshold in the BES definition are timely registered with NERC and evaluated for BES Cyber System identification and categorization.
2. CIP-002-5.1a, R1: Ensure that all affiliate and third-party cyber systems used to monitor and control BES generation resources are considered by Generator Operators (GOPs) as part of their BES Cyber System identification and categorization procedures.¹⁶
3. CIP-004-7, R4, R5 and R6: Ensure that super intelligence (SI) tools' (SI tools) access to BES Cyber Systems and BES Cyber System Information is authorized.

16 NERC defines BES Cyber System as “[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.” In turn, BES Cyber Asset is defined as “[a] Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System....” See NERC Glossary of Terms Used in Reliability Standards.

Timely Registration and CIP Compliance for Generation Resources¹⁷

OVERVIEW

Pursuant to Reliability Standard CIP-002-5.1a, R1, all generation resources that are synchronized to the BES and generating power greater than the applicable threshold in the BES definition should be timely registered with NERC and evaluated for BES Cyber System identification and categorization.

Audit staff observed that some entities did not timely register with NERC as new generator owners and consequentially did not conduct a review to identify BES Cyber Systems pursuant to Reliability Standard CIP-002-5.1a, Requirement R1. Other entities registered with NERC but did not conduct a timely review pursuant to CIP-002-5.1a, Requirement R1.

BACKGROUND

All entities that are users, owners or operators of the Bulk-Power System, and that perform a reliability function as set forth in NERC's Statement of Compliance Registry Criteria, and either meet the NERC definition of BES or are otherwise determined to have a material impact on the reliable operation of the Bulk-Power System are required to register with NERC.¹⁸ Registered entities are responsible for compliance with the requirements in the FERC-approved Reliability Standards applicable to the specific reliability function performed by the registered entity.

Of particular relevance to this lesson learned, the NERC definition of bulk electric system Inclusion I2 provides: "Generating Resource(s) including the generator terminals through the high side of the step-up transformer(s) connected at a voltage of 100 kV or above with: (a) Gross individual nameplate rating greater than 20 MVA. Or, (b) Gross plant/facility aggregate nameplate rating greater than 75 MVA."¹⁹ Further, the NERC Statement of Compliance Registry Criteria defines a Generator Owner as "[t]he entity that: 1) owns and maintains generating Facility(ies) (Category 1 GO); or 2) owns and maintains non-BES inverter-based generating resources that either have or contribute to an aggregate nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV (Category 2 GO)."²⁰

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 Reliability Standard CIP-002-5.1a'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.

17 Previous lessons learned reports have also discussed inconsistencies in the identification of generation resources in different contexts. See *2025 Lessons Learned from Commission-Led CIP Reliability Audits*, at 5 (lesson #1); and *2017 Staff Report Lessons Learned from Commission-Led CIP Version 5 Reliability Audits*, lesson #3; *2017 Staff Report Lessons Learned from Commission-Led CIP Version 5 Reliability Audits*, at 10 (lesson #3).

18 See NERC Rules of Procedure, App. 5B (Statement of Compliance Registry Criteria), at 1 (effective June 27, 2024).

19 See NERC Glossary of Terms Used in Reliability Standards, www.nerc.com/glossary-of-terms.

20 NERC Rules of Procedure, App. 5B at 5.

AUDIT OBSERVATION

Audit staff found that some entities did not timely: (1) register with NERC for new generation resources and (2) identify and categorize new generation resources pursuant to Reliability Standard CIP-002-5.1a R1. Audit staff observed multiple instances in which an inverter-based resource (IBR) was synchronized to the BES, had achieved commercial operation beyond initial testing, and was producing an aggregate amount of generating resource(s) (gross nameplate rating) that was greater than the applicable threshold in the BES definition, yet its associated cyber systems were not identified and categorized as BES Cyber Systems. In some instances, the owners and operators of these generation resources were not yet registered with NERC and therefore had not conducted a review to identify and categorize BES Cyber Systems as required by Reliability Standard CIP-002-5.1a. In other instances, the owners and operators were already registered with NERC and subject to the CIP Reliability Standards, but they had not yet evaluated their generation resources under the Reliability Standard CIP-002-5.1a impact rating criteria.

Audit staff observed that, in both scenarios, the failure to conduct a timely evaluation under Reliability CIP-002-5.1a stemmed from entities' misunderstanding or unawareness of NERC's definition of the term Commercial Operation Date (COD).

NERC's Enterprise Registration Procedure defines COD as "the date after which all initial testing and commissioning has been completed and is the initiation date on which the Generator Owner and Generation Operators can start producing electricity for sale."²¹ NERC further explains that:

Generation resources . . . that initiate commercial operations in stages or phases are required to register when the generation resources (synchronous generators, wind turbines, solar PV, battery storage, etc.) achieve Commercial Operation for an aggregate amount of generating resource(s) (gross nameplate rating) that is greater than the applicable threshold. The entity should initiate the registration process when this occurs so that the effective registration date coincides with the COD for that phase of the generation resource that exceeds the applicable threshold. Upon the effective registration date, all generating resources are expected to be 100% compliant with all applicable Reliability Standards.²²

Audit staff noted that some entities misunderstood the appropriate COD for NERC registration and compliance. Several generator owners indicated that they had multiple CODs associated with phased implementation of generation resources while in generator interconnection queues of organized electric markets and would wait until they had achieved full nameplate capacity and had completed all phases of the generator interconnection queue before considering NERC registration and CIP-002 evaluation. For example, one entity was synchronized to the BES, completed all initial testing and commissioning, and achieved commercial operation for an aggregate amount of generating resource(s) (gross nameplate rating) that was greater than the applicable threshold for over a year, yet it delayed NERC registration until it had completed all phases of the generator interconnection queue of an organized electric market and had achieved commercial operation of the resource's full nameplate capacity. An entity actively attempting to comply with its interconnection obligations may nonetheless inadvertently neglect its cybersecurity requirements or not timely comply.

21 NERC, *ERO Enterprise Registration Procedure* at 16 (Jun. 11, 2026), www.nerc.com/globalassets/programs/registration/registration-documentation/ero-enterprise-registration-procedure.pdf.

22 *Id.* at 3 (internal footnote omitted).

RISK

Timely identification and categorization of BES Cyber Systems under CIP 002 5.1a is essential. The accurate identification of BES Cyber Systems pursuant to CIP-002-5.1a is the cornerstone of the CIP Reliability Standards because it provides a risk-based criteria for determining how a responsible entity must comply with the remaining CIP requirements. Delays can result in misapplied or missing security controls, increasing exposure to vulnerability and potential risk of compromise, and heightening risk to the reliable and secure operation of the BES.

MITIGATION

Generation owners and generation operators should apply the NERC definition of COD to determine the appropriate timing for registration and compliance with mandatory Reliability Standards. Entities that own a generation resource that meets the registration criteria should ensure timely: (1) registration of their resources with NERC and (2) identification and categorization of BES Cyber Systems and associated BES Cyber Assets under CIP 002 5.1a. Entities that are already registered with NERC must review their generation resources to identify and categorize the BES Cyber Systems and associated BES Cyber Assets under CIP-002-5.1a.

Identify and Categorize All BES Cyber Systems Used for Generation Operation

OVERVIEW

Pursuant to CIP-002-5.1a, R1 all affiliate and third-party cyber systems used to monitor and control BES generation resources should be considered by Generator Operators as part of their BES Cyber System identification and categorization procedures.

Audit staff observed circumstances in which affiliate companies and third-party contractors exercised monitoring and control of generation resources that could have a material impact on the reliability of the Bulk-Power System.

BACKGROUND

Reliability Standard CIP-002-5.1a, Requirement R1 requires registered entities to identify and categorize BES Cyber Systems and their associated BES Cyber Assets used to monitor and control BES generation resources. Correctly identifying and categorizing BES Cyber Systems allows for the proper 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 are classified as low, medium, or high impact.

AUDIT OBSERVATIONS

Audit staff identified two circumstances where an unregistered entity performed (or had the capability of performing) generation monitoring and control functions at an aggregation point, i.e., generation control center, on behalf of multiple registered GOPs. In both circumstances, while the individual GOP identified one or more low impact BES Cyber Systems, the aggregate monitoring and control function performed by the unregistered entity satisfied the rating criteria for a medium impact BES Cyber System pursuant to Reliability Standard CIP-002-5.1a and thus had increased compliance responsibility.²³

In the first circumstance, staff observed corporate structures with a parent company that was not registered for any function and multiple affiliated companies each separately registered as a GOP. Each individual affiliated company categorized its BES Cyber Systems as low impact. However, the parent company maintained generation monitoring and control capability at a single control center of affiliated companies' generation resources that in aggregate were commensurate with a medium impact rating.

In the second circumstance, staff observed that multiple *unaffiliated* GOPs contracted with the same third party (e.g., vendor, contractor, or service provider) to perform monitoring and control of generation resources. Similar to the first circumstance, the individual registered GOPs each identified their BES Cyber Systems as low impact. However,

23 See Reliability Standard CIP-002-5.1a, Att. 1, Section 2.1 (medium impact rating for “[c]ommissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection).

the third party collectively provided generation monitoring and control for the multiple generation resources that in aggregate were commensurate with a medium impact rating.

In both circumstances, affiliate companies and third parties exercised monitoring and control of generation resources that could have a material impact on the reliability of the Bulk-Power System. Audit staff raised the above concerns yet registered entities were reluctant to discuss affiliate company or third-party monitoring and control capabilities.

RISK

Failure to properly identify and categorize BES Cyber Systems under CIP-002-5.1a exposes registered entities to significant reliability and security risks, through the application of insufficient or missing security controls which results in inadequate protection of BES Cyber Systems. As control capabilities become more diverse, remote, and complex, identifying and categorizing BES Cyber Systems used for generation operation needs to evolve to ensure cyber systems, individually or in aggregate, are identified and classified commensurate with the risk of their loss, compromise, or misuse. When BES Cyber Systems are not accurately identified and categorized with the correct impact rating, an entity might fail to implement the appropriate controls that would prevent or mitigate adverse effects on the reliable operation of the Bulk-Power System.

In the two circumstances above, the registered entities failed to account for the aggregation of their, and other parties', cyber assets. As a result, their assets (the assets of the third-party) were categorized as low impact, rather than medium impact and not subject to the increased requirements for medium impact facilities.²⁴

MITIGATION

Identification and categorization of BES Cyber Systems is the foundation of the CIP Reliability Standards. Proper identification and categorization ensure that the appropriate level of associated controls is applied commensurate with the impact rating and risk a system poses to reliability and security of the Bulk-Power System. Demonstrating compliance with the CIP Reliability Standards for all cyber systems that should be categorized as BES Cyber Systems, including those operated by an affiliate or third party, is the responsibility of all GOPs.²⁵

That being said, NERC should consider providing further guidance or modifications to Reliability Standards or registration procedures to adequately address the specific circumstances observed by the auditors. Housing control of multiple generation resources at a single location with a *de facto* operator enhances the cybersecurity risk, and NERC should consider appropriate action.

24 BES Cyber Systems classified as medium impact are subject to the full suite of CIP cybersecurity controls, which currently includes approximately 140 requirements and sub-requirements, while those classified as low impact are subject to a limited, primarily plan-based subset of approximately 15 requirements, reflecting their lower reliability impact and reduced mandatory controls.

25 See *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, 118 FERC ¶ 61,218, at P 144, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007) ([T]here is a difference between being assigned to perform a task and being responsible for completing the task. The organization that registers with NERC to perform a function will be the responsible entity and, while it may delegate the performance of that task to another, it may not delegate its responsibility for ensuring the task is completed.”).

Access to BES Cyber Systems and BES Cyber System Information Facilitated by SI Tools

OVERVIEW

CIP-004-7, R4, R5 and R6 requires access to BES Cyber Systems and BES Cyber System Information facilitated by super intelligence (SI) tools be authorized.

Audit staff has observed that SI tools have become more deeply embedded in CIP-networked environments, offering significant efficiencies in automating routine cybersecurity tasks and streamlining analysis workflows; however, their rapid adoption has introduced new and evolving risks that entities must proactively assess and manage.

BACKGROUND

Reliability Standard CIP-004-7, Requirement R4 requires registered entities to have a documented process “to authorize based on need, as determined by the Responsible Entity...” for electronic access to high- and medium-impact BES Cyber Systems.²⁶ Further, once electronic access is granted, the registered entity must periodically verify that the electronic access remains necessary. Reliability Standard CIP-004-7, Requirement R5 requires registered entities to timely revoke, when necessary, a user’s electronic access to high- and medium-impact BES Cyber Systems. Reliability Standard CIP-004-7, Requirement R6 requires registered entities to authorize, regularly verify, and timely revoke a user’s provisioned access, as the need arises, to BES Cyber System Information (BCSI).

While most entities have mature access control programs and methods in place, the introduction and evolution of SI tools has presented new and evolving challenges in ensuring sufficient access control.

AUDIT OBSERVATIONS

Audit staff observed increased adoption of SI tools across registered entities’ CIP-networked environments. While audit staff found that registered entities generally accounted for the use of SI tools in their CIP-networked environment and applied appropriate controls, audit staff observed variations in how entities addressed SI access.

SI tools offer useful tools for registered entities, including machine learning to adapt to new situations and the ability to optimize their performance over time. Currently, most SI tools are limited to chatbots, which answer questions, and personal assistants, which organize schedules or draft emails. However, SI tools are becoming more sophisticated, monitoring communication networks, reacting to threats, and providing operations similar to users.

During audit interviews, entities identified both potential SI use cases and risks associated with deploying SI tools in CIP-networked environments. Specifically, entities communicated that, while many vendors and suppliers now add SI tools to their products and services, compliance programs are slow to adapt to address these risks. Entities noted that the growing sophistication of SI capabilities may enable these tools to perform actions that mimic user behavior, increasing the difficulty of distinguishing legitimate activity from malicious use that complicates detection and response efforts. If not properly monitored and controlled, SI tools may introduce unanticipated lateral-movement vectors or enable unauthorized access to BES Cyber Systems and BES Cyber System Information. Further, audited

26 Reliability Standard CIP-004-7, Requirement R4.1

entities indicated that the scope and ability of SI tools may not be fully understood until after the products or services are active on an entity's network, resulting in access control risks.

RISK

As SI tools become increasingly prevalent in all software, their integration into BES Cyber Systems products and solutions is becoming commonplace. Because these tools may have unrestricted access across systems, they have emerged as attractive targets for adversaries. As NERC identifies in its CIP Roadmap, the targeting of SI tools is an emerging risk registered entities must be cognizant of while deploying these tools within a CIP environment.²⁷ Recent real-world intrusions show that, if not properly protected, adversaries can leverage commercially available SI tools that reside on entity systems to map environments, identify pathways toward critical systems, accelerate reconnaissance, and automate exploitation attempts.

MITIGATION

While the CIP Reliability Standards do not explicitly allow or prohibit the use of SI tools, entities should consider the risks those tools pose when evaluating their BES Cyber Systems and apply the appropriate controls accordingly. First, entities should consider the business need for deploying SI tools within a CIP-networked environment. Further, entities should properly grant, regularly verify, and timely revoke users' electronic access to BES Cyber Systems and BCSI that is facilitated by SI tools, per Reliability Standard CIP-004. In addition, entities should consider the following:

1. Ensure all SI tools' access to communications outside the CIP-005 electronic security perimeter are understood and monitored, including the reason for granting access.²⁸
2. Identify and inventory SI tools as a generic service accounts per Reliability Standard CIP-007; and ensure that default passwords, if applicable, are changed.²⁹
3. Limiting an SI tool's ability to access BCSI per Reliability Standard CIP-011.³⁰
4. Identify and assess the risks from SI products or services from prospective vendors as a part of their CIP-013 supply chain risk management plan³¹ Entities should use a risk management framework, such as NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)³² when implementing SI within their networks.³³

27 See NERC, *Critical Infrastructure Protection Roadmap: 2025 NERC Work Plan Priority* (Jan. 2026) (CIP Roadmap), www.nerc.com/globalassets/our-work/reports/special-reports/nerc_cip_roadmap_01122026.pdf.

28 Under Reliability Standard CIP-005 (Cyber Security – Electronic Security Perimeter), registered entities must protect BES Cyber Systems against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System.

29 Under Reliability Standard CIP-007 (Cyber Security — System Security Management), registered entities must manage system security by implementing select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System. The Standard states that a “generic account” is a “group account set up by the operating system or application to perform specific operations.”

30 Under Reliability Standard CIP-011 (Cyber Security — Information Protection), registered entities must prevent unauthorized access to BES Cyber System Information by implementing information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System.

31 *Under Reliability Standard CIP-013 (Cyber Security – Supply Chain Risk Management), registered entities must mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems.*

32 NIST AI 800-2 is currently in draft format.

33 See NIST, *NIST AI 100-1 Artificial Intelligence Risk Management Framework* (AI RMF 1.0) (Jan. 2023), nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.



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

FERC.GOV