



FERC Cybersecurity Updates & Lessons Learned

Alan Herd, Deputy Director

Division of Cyber Security

Office of Electric Reliability

The views expressed in this presentation are my own and do not represent those of the Commission or any individual Commissioner



Division of Cyber Security

- The Division of Cyber Security is in the Office of Electric Reliability at FERC.
- Our primary responsibility is to oversee implementation of the Critical Infrastructure Protection Reliability Standards (CIP Standards).
 - Monitor and participate in the CIP Standards development process
 - Analyze proposed modified or new CIP Standards
 - Oversee and independently perform compliance monitoring of the CIP Standards
 - Track and review all noncompliance with the CIP Standards



Cybersecurity Update

- Internal Network Security Monitoring (CIP-015)
 - Order No. 907 (June 2025) and 907-A (August 2025)
- Supply Chain Risk Management (CIP-013)
 - Order No. 912 (September 2025)
- Security Controls for Low-Impact Systems (CIP-003)
 - Order No. 918 (March 2026)
- Virtualization Reliability Standards Modifications
 - Order No. 919 (March 2026)



FERC-led Cybersecurity Audits

- FERC staff has been conducting cybersecurity audits since 2016.
 - Evaluate compliance with the CIP Standards
 - Identify cybersecurity risks
 - Inform CIP Standards development efforts
- FERC issues an annual anonymized summary report that informs the regulated community and the public of lessons learned from the previous year's audits.



Lessons Learned Reports

- <https://www.ferc.gov/staff-reports-and-papers>
- Click on the “Lessons Learned” tab:

www.ferc.gov/staff-reports-and-papers

ERO Enterprise | FERC | Government | News | Reference | Vendor | SharePoint | Document Draftin... | PMU Update | The Fed - Distribut...

Resources

- Overview
- Reports and Papers**
 - Peer Review
 - Reports to Congress
- Guides
- The Process
- Corporate Officials
- Public Reference Service
- Transmission Line Vegetation Management
- Open Data Portal

Staff Reports and Papers

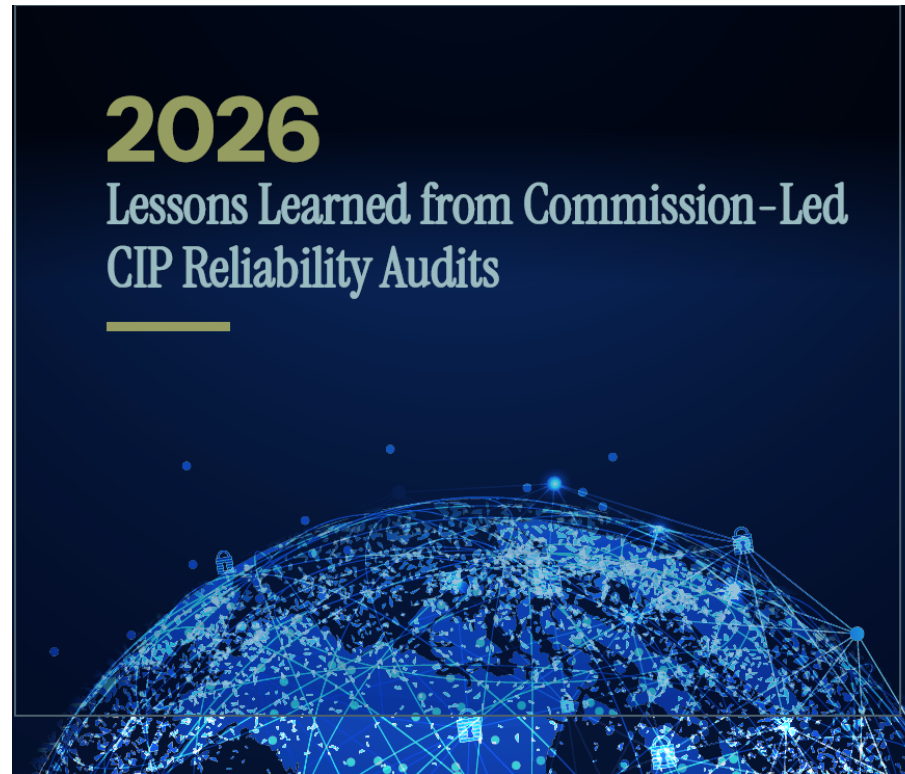
Each year, the Commission's Staff makes public various docketed and non-docketed reports that are primarily of an investigative and informational nature. Click on the categories below to view additional information.

General | Electric | Natural Gas | Hydropower | Oil | Energy Infrastructure | Staff Papers | **Lessons Learned**

Issuance Date	Title
October 20, 2025	2025 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits
August 26, 2024	2024 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits News Release
December 12, 2023	2023 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits News Release
October 14, 2022	2022 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits News Release
October 8, 2021	2021 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits News Release
	2008 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits



2026 Lessons Learned Report



<https://www.ferc.gov/news-events/news/ferc-staff-report-offers-lessons-learned-2026-cip-audits>

Lessons from 2026 Audits

1. Timely Registration and CIP Compliance for Generation Resources
2. Identify and Categorize All BES Cyber Systems Used for Generation Operation
3. Access to BES Cyber Systems and BES Cyber System Information Facilitated by Super Intelligence (SI) Tools



Generation Resources

- 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.



Generator Operators

- 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.
- 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.



Super Intelligence

- Audit staff observed increasing use of super intelligence (SI) tools, including chatbots, personal assistants, and automated analytical systems, within CIP-networked environments.
- 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.

