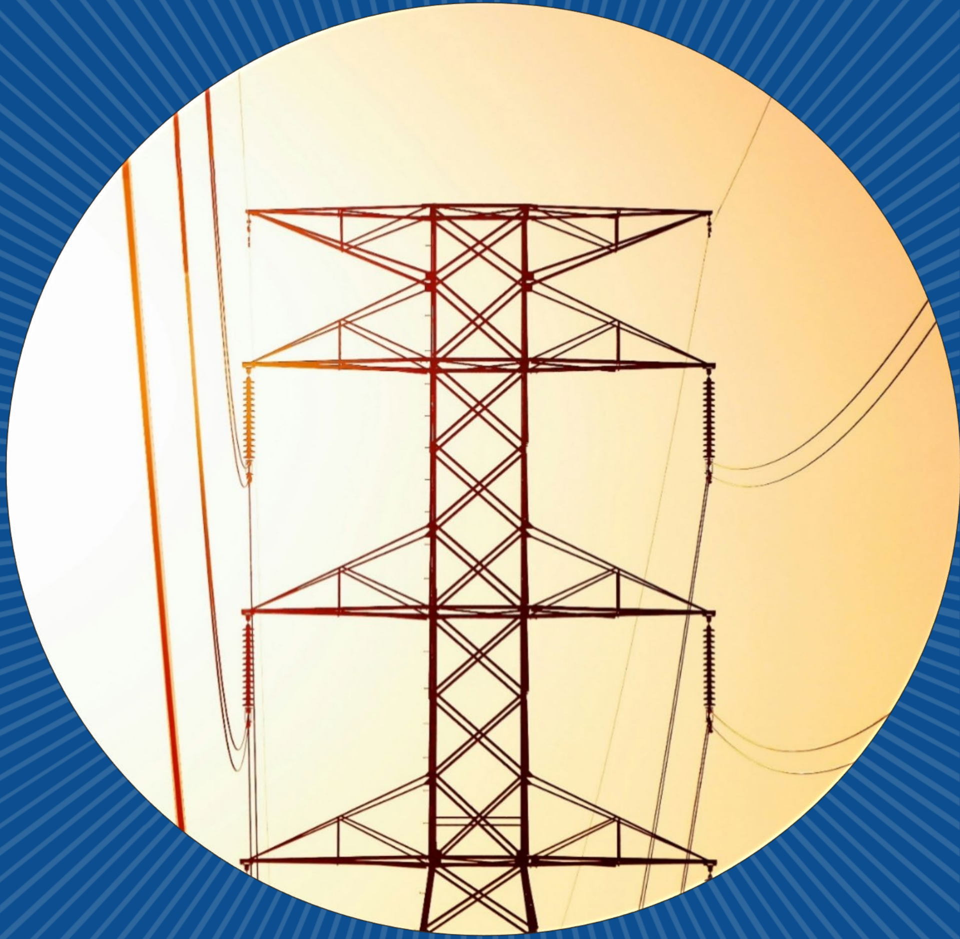
NPCC

FERC Lessons Learned Report (LLR)

Joshua Okoniewski
Senior CIP Analyst

March 10, 2026



NPCC Outreach, Training, Events Disclaimer

Northeast Power Coordinating Council, Inc. (NPCC) is committed to providing outreach, training, and nonbinding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from NPCC's organizational groups and the industry may develop materials, including presentations, provided as part of the event. The views expressed in the event materials are those of the SMEs and do not necessarily express the opinions and views of NPCC.

Antitrust Compliance Guidelines

Because this event brings together market participants who may be viewed as actual or potential competitors, we must be mindful to conduct it in a manner that is consistent with the antitrust and competition laws. Participants should not disclose non-public, proprietary, or competitively sensitive information.

Attendees should exercise independent judgment and avoid even the appearance of discussions of agreements or concerted actions that may be viewed as restraining competition. Any company decisions that are informed by your discussions today must be made independently.

This guidance is not intended as legal advice, and each attendee is responsible for seeking their own legal advice with respect compliance with applicable antitrust and competition laws. However, any questions on NPCC's Antitrust Policy may be directed to NPCC's General Counsel.

Webinar Housekeeping

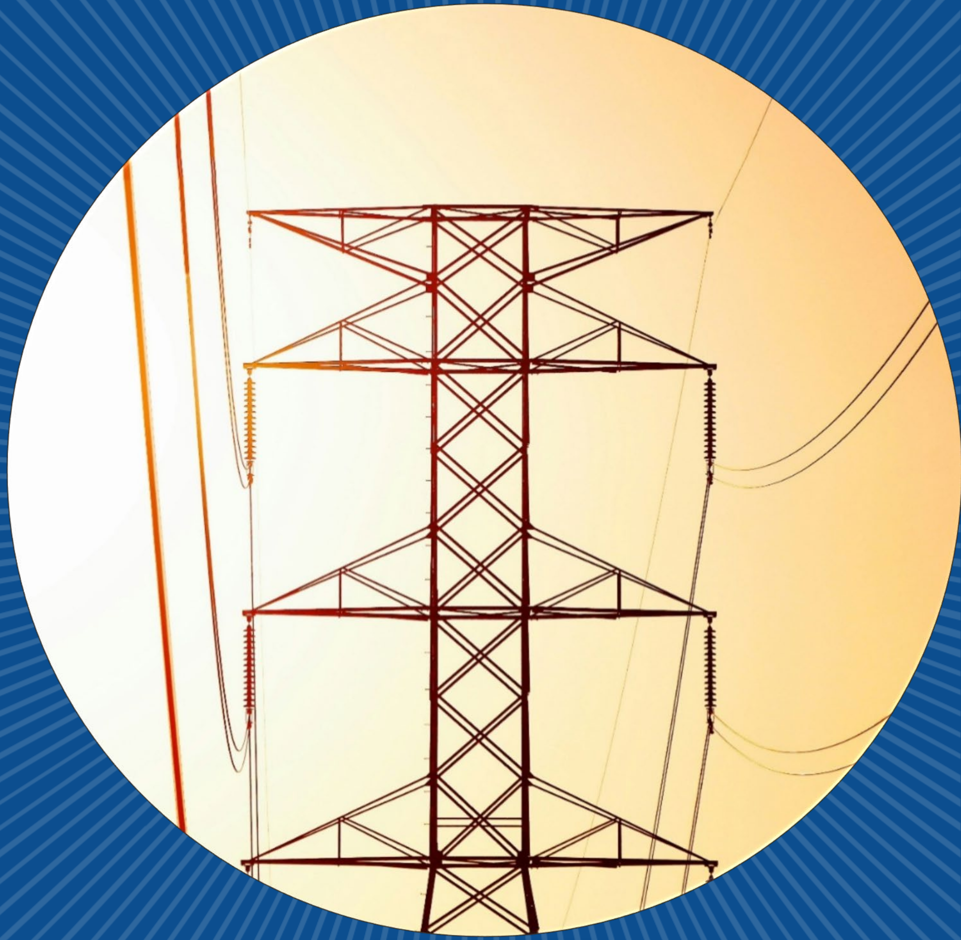
Recording: This webinar is being recorded. A link to the recording will be shared with all registrants after the session, so you can revisit the content or share it with colleagues.

Audio: All participants are muted by default to minimize background noise. If you experience any audio issues, try refreshing your browser or checking your device settings.

Q&A: We encourage your questions! Please use the Q&A box at the top of your screen to submit questions at any time. We'll address as many as we can during the Q&A portion at the end.

NPCC

FERC Lessons Learned Report (LLR)



Joshua Okoniewski

Senior CIP Analyst

March 10, 2026

Agenda

- Overview (Background of LLR)
- CIP Standards Addressed
- Lesson 1
- Lesson 2
- Lesson 3
- Summary
- Additional Resources
- Questions

Overview

- 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 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.

CIP Standards Addressed

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.

Lesson 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.

Lesson 1

Overview: 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.

Risk: 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.

Best Practices for Risk Reduction

Asset Classification: Ensure all assets are properly classified (review of CIP-002 categorization).

MW Threshold: Ensure MW threshold includes non-BES assets in total MW threshold. Both BES and non-BES assets must be included in the MW threshold.

CIP-002 Evaluation Study: Ensure proper CIP-002 evaluation is done for assets regarding a 15-minute impact.

Lesson 2:
CIP-003-8, CIP-006-6, CIP-010-4

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

Lesson 2

Overview: 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.

Risk: 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.

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

Best Practices for Risk Reduction

Compliance Oversight: Understand what is being done to meet the compliance obligations. Third parties may not be aware of the compliance requirements.

What agreements are in place?: Ensure that agreements are in place with the third parties to meet the compliance obligations.

Health Checks: Periodically check on the status of projects or duties that are assigned to third parties to ensure compliance obligations are being met.

Lesson 3: CIP-004-7, CIP-010-4

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

Lesson 3

Overview: 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. 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.

Risk: 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, it is unlikely that entities can provide the measures needed to demonstrate compliance with the relevant Reliability Standards.

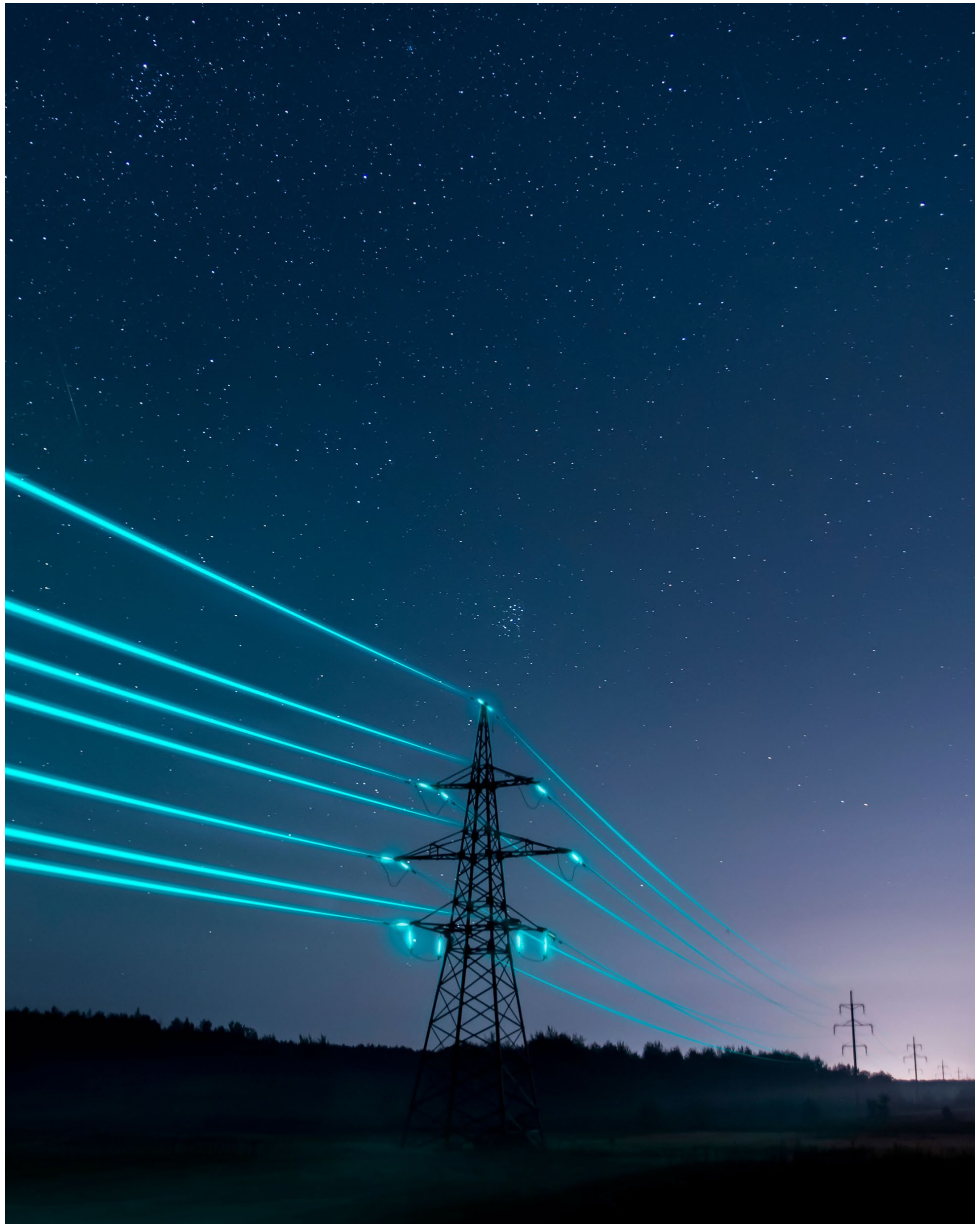
Mitigation: In general, it is a strong cyber security practice to consider both benefits and risks when deciding whether to use cloud services. Registered entities should understand the current limitations of the CIP standards have when operating high and medium impact BES cyber systems in the cloud. 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.

Best Practices for Risk Reduction

Memorandum of Understanding (MOU): Understanding what MOUs are in place when acquiring Cloud Services that could impact compliance.

Who has access?: When using a Cloud Service provider who has access to sensitive information to ensure that compliance is met.

What standards are implicated: Understand when using a Cloud Service Provider that some CIP standards could fall under the umbrella of service they are providing.



Summary

- The Commission initiated its Reliability Standards audit program for registered entities in FY2016, and the Commission has conducted CIP Audits each year since.
- The Commission has published previous lessons learned and summarized them in the final report each year dating back to 2017.
- This report does not cover all issues discovered on FERC audits but provides details around specific areas the Commission focused on.

Additional Resources

FERC
Order No. 2222
www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf
NOTE: See PP 114 and page 93.

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

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

FERC Staff Report Offers Lessons Learned from 2025 CIP Audits
https://www.ferc.gov/news-events/news/ferc-staff-report-offers-lessons-learned-2025-cip-audits

NPCC

Questions?

Contact Us: npcc.org/contact

Compliance Monitoring CIP Team
Joshua Okoniewski CIP Senior Analyst

March 10, 2026

Upcoming NPCC Events

Upcoming Standards Webinar	• March 24, 2026 • 10:00 – 11:00 am • Register
Reliability Forum	• March 26, 2026 • 9:00 am – 12:00 pm • Register
NPCC Spring 2026 Compliance and Reliability Webinar	• May 20, 2026 • 9:00 am – 12:00 pm • Registration Link coming
NPCC Fall 2026 Hybrid Compliance and Reliability Conference	• November 4 - 5, 2026 • Newport Marriott Hotel & Spa Newport, RI • Registration Link coming