Update on FERC Activities

Kal Ayoub, Deputy Director, Division of Cyber Security

October 24, 2022

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

Reliability - Related Activity

- OER Deputy Director Announcement
- Joint Federal–State Task Force on Electric Transmission
- Upcoming Technical Conferences
- Extreme Weather Actions
- Proposed Rule on Transmission Planning
- NOPR on Incentives for Voluntary Cybersecurity Investments
- 2022 Report on Lessons Learned from the FERC-led Cybersecurity Audits

Eric Vandenberg, OER Deputy Director 10/24/22

- Eric first joined the Commission in 2009 as an Electrical Engineer in the Office of Electric Reliability.
- Eric has served as Deputy Director of the Office of Energy Policy and Innovation (OEPI) since December 2019.
- Prior to his appointment in OEPI, Eric served as a Technical Advisor to former Chairman Chatterjee, and also as a Group Manager in the Office of Energy Market Regulation (OEMR).
- Eric received his Bachelor of Science in Electrical Engineering and Master of Business Administration from Ohio University.

Joint Federal-State Task Force on Electric Transmission

- ***Announced*** (June 17, 2021, in Docket No. AD21-15). The Joint Federal-State Task Force's purpose is to encourage cooperation and communication between federal and state regulators on electric transmission related issues.
- ***The First meeting*** (November 10, 2021) focused on incorporating state perspectives into regional transmission planning.
- ***The Second meeting*** (February 16, 2022) focused on categories and types of transmission benefits that should be considered in transmission planning and cost allocation and its principles.
- ***The Third meeting*** (May 6, 2022) focused on examining barriers to the efficient, expeditious, and reliable interconnection of new resources through the FERC-jurisdictional interconnection processes.
- ***The Fourth meeting*** (July 20, 2022) focused on Interregional Transmission Planning and Project Development
- ***The Fifth meeting*** (November 15, 2022)
- Recording are available on the Joint Federal-State Task Force website.

Upcoming Technical Conferences

- **Annual Commissioner-led Reliability Technical Conference** will be held on November 10, 2022. AD22-10-000. The conference will discuss policy issues related to the reliability and security of the Bulk-Power System. Panel I will explore Managing the Electric Grid to Advance Reliability; and Panel II will explore Managing Cyber Security Threats, CIP Reliability Standards and best practices for the Bulk-Power System.

- **Establishing Interregional Transfer Capability Transmission Planning and Cost Allocation Requirements Workshop** will be held on December 5-6, 2022. AD23-3-000. The workshop will discuss whether and how the Commission could establish a minimum requirement for interregional transfer capability for public utility transmission providers in transmission planning and cost allocation processes.

- ***Supply Chain Risk Management Technical Conference*** will be held on December 7, 2022. AD22-12-000. DOE's Office of Cyber Security, Energy Security, and Emergency Response (CESER) and FERC's Office of Electric Reliability will hold a technical conference to discuss supply chain security challenges related to the Bulk-Power System, ongoing supply chain-related activities, and potential measures to secure the supply chain for the grid's hardware, software, computer, and networking equipment.

Extreme Weather Actions

Extreme weather has impacted the electric grid throughout its history. The severity and frequency of extreme weather events is increasing. To address this issue, the Commission took the following actions:

- Hosted a Joint FERC, NERC and Regional Entities Technical Conference on Improving Winter-Readiness of Generating Units (April 27 & 28, 2022), Docket No. AD22-4-000.
- Issued a NOPR on Transmission System Planning Performance Requirements for Extreme Weather (June 16, 2022), Docket No. RM22-10-000.
- Issued a NOPR on One-Time Informational Reports on Extreme Weather Vulnerability Assessments Climate Change, Extreme Weather, and Electric System Reliability (June 16, 2022), Docket Nos. RM22-16-000 and AD21-13-000.

NOPR on Transmission Planning Performance Requirements

- June 16, 2022 – Transmission Planning Performance Requirements for Extreme Weather, Docket No. RM22-10-000.
  - ✓NOPR addresses improving the reliability of the bulk power system to counter the risks presented by extreme weather.
  - ✓NOPR proposes to direct NERC to develop modifications to reliability standard TPL-001-5.1 to account for the risks of extreme heat and cold conditions. The NOPR also seeks comment on whether to require studies and corrective action plans for drought conditions.
  - ✓Comments were due August 26, 2022.
  - ✓32 number of comments received

NOPR on Incentives for Voluntary Cybersecurity Investments

- September 22, 2022, Docket No. RM22-19-000.
- In the Infrastructure Investment and Jobs Act of 2021, Congress directed FERC to revise its regulations to establish incentive-based rate treatments by encouraging utilities to invest in advanced cybersecurity technology and participate in cybersecurity threat information sharing programs.

NOPR on Incentives for Voluntary Cybersecurity Investments

- Cybersecurity expenditures would be:
  - Eligible for an incentive including both expenses and capital investments associated with advanced cybersecurity technology and participation in a cybersecurity threat information sharing program.
  - Would be voluntary and have to materially improve the utility's cybersecurity posture. FERC proposes to establish a pre-qualified (PQ) list of cybersecurity expenditures that are eligible for incentives that would be publicly maintained on the FERC.gov website.
- The incentives would take two forms: a return on equity adder of 200 basis points, or deferred cost recovery that would enable the utility to defer expenses and include the unamortized portion in its rate base.
- Approved incentives, with certain exceptions, would remain in effect for up to five years from the date on which the investments enter service or expenses are incurred.
- Comments due November 7, 2022.

Lessons Learned Report – Background

- A staff report derived from the Commission's nonpublic CIP compliance audits conducted over the previous fiscal year.
- Issued publicly on an annual basis to help entities assess cybersecurity risk and compliance with mandatory reliability standards and, more generally, facilitate efforts to improve the security of the nation’s electric grid.
- Contains recommendations to help users, owners, and operators of the BPS improve their compliance with the CIP Standards and their overall cybersecurity posture.

Lessons Learned Report – Background

- The CIP audits are conducted by OER staff, with assistance from OE staff.
  - Regional Entity and NERC staff actively participate on the audits and have access to all evidence.
- The Lessons Learned Reports are developed collaboratively by OER and OEIS staff.
- Six (6) annual reports with a total of 69 lessons issued to date:
  - 2022 Report (5 lessons learned)
  - 2021 Report (14 lessons learned)
  - 2020 Report (12 lessons learned)
  - 2019 Report (7 lessons learned)
  - 2018 Report (10 lessons learned)
  - 2017 Report (21 lessons learned)

Lessons Learned from CIP Reliability Audits

FERC staff issued its annual report on lessons learned from the non-public CIP audits of registered entities. It found that most cybersecurity protection measures adopted by entities met the mandatory requirements of the CIP reliability standards.

The report recommends cybersecurity practices that include processes, procedures and technical controls to mitigate risks.

Recommendations include:

- Re-evaluate policies, procedures, and controls for low-impact cyber systems and associated cyber assets (CIP-003);
- Address risks posed by bulk electric system cyber assets that have reached the manufacturer-determined end of life or service and no longer are supported by vendors (CIP-007);
- Deploy a comprehensive malicious code prevention program for all cyber assets within a bulk electric system cyber system (CIP-007);
- Implement comprehensive vulnerability assessment processes for applicable cyber assets (CIP-010); and
- Review and validate controls used to mitigate software vulnerabilities and malicious code on transient cyber assets managed by a third party (CIP-010).

Questions?