Highlights of the 2021 Report on Lessons Learned from the FERC-led Cybersecurity Audits

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.
- Five (5) annual reports with a total of 64 lessons issued to date:
  - 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)

2021 Lessons Learned Report

CIP-002

- Enhance policies and procedures to include evaluation of Cyber Asset misuse and degradation during asset categorization.

CIP-003

- Properly document and implement policies, procedures, and controls for low impact Transient Cyber Assets (TCAs).

CIP-004

- Implement a defined workflow to enhance processes for the verification of electronic access, unescorted physical access, and access to BES Cyber System Information (BCSI).
- Base access to BCSI on “need to know.”

2021 Lessons Learned Report

CIP-007

- Enhance physical and logical port protection controls for Cyber Assets.
- Review the system access control program periodically to ensure processes and procedures are implemented as documented.

CIP-009

- 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 Lessons Learned Report

CIP-010

- Review configuration change management processes periodically and ensure that they are implemented properly.
- Enhance configuration change management procedures and controls to document and account for differences between test and production environments.
- Improve vulnerability assessments to include credential-based scans of Cyber Assets.
- Properly document and implement policies, procedures, and controls for medium and high impact TCAs.

2021 Lessons Learned Report

CIP-011

- Enhance policies and procedures to include BCSI spillage investigation and response.
- Enhance policies, procedures, and controls to properly track, document and monitor BCSI storage locations.

Internal Controls

- Enhance internal compliance and controls programs to include control documentation processes and associated procedures pertaining to compliance with the CIP Reliability Standards.