Cybersecurity Updates and Audits Lessons Learned Report

Federal Energy Regulatory Commission | Washington D.C.

Order No. 850, Order No. 848, CIP-012-1 NOPR and Audits Lessons Learned Report Update

Patricia Eke
Energy Industry Analyst
Office of Electric Reliability

September 25, 2019

Disclaimer

The views expressed herein are mine, and do not necessarily reflect the views of the Commission, individual Commissioners, Commission staff, or individual Commission staff members

Supply Chain Risk Management Reliability Standard (Order No. 850)

❑ Approved by the Commission: October 18, 2018

❑ Commission approved three Reliability Standards ("Supply Chain Standards") to mitigate cybersecurity risks associated with the supply chain for BES Cyber Systems.

❑ Supply Chain Standards becomes effective July 1, 2020

Supply Chain Risk Management Reliability Standard (Order No. 850)

- ❑ Supply Chain Standards Requirements:
  - ❑ Requires entities to develop, implement and review a supply chain cyber security risk management plan(s)
  - ❑ Requires entities to be aware of all active vendor remote access sessions taking place on the entity’s system
  - ❑ Verify software integrity and authenticity to ensure that software being installed was not modified without awareness of the software supplier and is not counterfeit

Supply Chain Risk Management Reliability Standard (Order No. 850)

- ❑ Commission directed NERC to study certain categories of assets not currently subject to the Supply Chain Standards.
- ❑ On May 28, 2019, NERC filed Cybersecurity Supply Chain Risks: Staff Report & Recommended Actions
- ❑ Further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with External Routable Connectivity
- ❑ Formal data request issued: August 19,2019

Cyber Security Incident Reporting Standards (Order No. 848)

- ❑ Issued by the Commission: July 19, 2018
- ❑ Directed NERC to develop and submit modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system (BES).

Cyber Security Incident Reporting Standards (Order No. 848)

❑ NERC filed proposed Reliability Standard CIP-008-6 (Cyber Security – Incident Reporting and Response Planning Standard) on March 3, 2019

❑ Approved by Commission Letter Order (CLO) on June 20, 2019

❑ Reliability Standards CIP-008-6 becomes effective January 1, 2021

Cyber Security Incident Reporting Standards (Order No. 848)

❑ Consistent with the Commission’s directive, the approved standard also:

- Requires certain minimum information be included in the incident reports such as suspicious activity;
- Includes deadlines for submitting the incident reports; and
- Requires the incident reports to be sent to DHS-NCCIC, or its successor, in addition to the E-ISAC

CIP-012-1 – Cyber Security – Communications between Control Centers NOPR

- ❑ Issued by the Commission: April, 18, 2019
- ❑ Proposes to approve Reliability Standard CIP-012-1 (Cyber Security – Communications between Control Centers) submitted by NERC in response to a Commission directive in Order No. 822
- ❑ Proposes to direct NERC to modify the reliability standard to:
  - Require protections regarding the availability of communication links and data communicated between bulk electric system control centers
  - Clarify the types of data that must be protected
- ❑ Comments were due July 24, 2019

2018 CIP Audits Lessons Learned Report

- Staff report issued: March 29, 2019
- Recommendations from lessons learned during Commission-led CIP audits
  - Report based on audits conducted in FY18

- OER-Led CIP Reliability Standards Audits
  - Office of Enforcement assisted in conducting the audits
  - Office of Energy Infrastructure Security assisted with analyzing the data for the report

2018 CIP Audits Lessons Learned Report

- Second Annual Report
  - Previous 2017 report covered audits from FY16 and FY17

- 13 Recommendations, examples:
  - Consider implementing valid security certificates within the boundaries of BES cyber systems
  - Consider implementing encryption for Interactive Remote Access that is sufficiently strong
  - Consider replacing or upgrading “end-of-life” system components of an applicable cyber asset
  - Report can be found: https://www.ferc.gov/legal/staff-reports/2019/2018-report-audits.pdf

Questions?