NEW YORK STATE RELIABILITY COUNCIL
MEETING 223: November 9, 2017

Summary of FERC's Lessons Learned from FERC-Led Cyber Security (CIP) Audits

The next NPCC Board of Directors meeting is scheduled for December 6, 2017. The following is a summary of the FERC's Lessons Learned from FERC-Led CIP Audits.

a. Background

i. FERC has completed a number of CIP audits of several registered entities.

ii. The audits occurred between 2016 and 2017.

iii. FERC discovered potential non compliances.

iv. FERC also identified areas of improvement.

b. Summary

i. The FERC report provides information and recommendations to NERC, Regional Entities, and registered entities that FERC believes are useful in assessments of risk, compliance, and overall cyber security.

ii. There are a total of 21 lessons learned in the report.

iii. Example lessons learned from the report:

a. Ensure that all shared facility categorizations are coordinated between the owners of the shared facility through clearly defined and documented responsibilities for CIP Reliability Standards compliance.

b. Conduct a detailed review of physical key management to ensure the same rigor in policies and testing procedures used for electronic access is applied to physical keys used to access the Physical Security Perimeter (PSP).

c. Enhance procedures, testing, and controls around manual transfer of access rights between personnel accessing tracking systems, Physical Access Control Systems (PACS), and Electronic Access Control Monitoring Systems (EACMS) or, alternatively, consider the use of automated access rights provisioning.

d. Enhance processes and controls around the use of manual logs, such as using highly visible instructions outlining all of the parts of the requirement with each manual log, to consistently capture all required information.

e. Perform regular physical inspections of BES Cyber Systems to ensure no unidentified Electronic Access Points (EAPs) exist.

f. Review communication protocols between business units related to CIP operations and compliance, and enhance these protocols where appropriate to ensure complete and consistent communication of information.