1977-2017
CELEBRATING 40 YEARS
Federal Energy Regulatory Commission

NEWS RELEASE

October 6, 2017
News Media Contact
Craig Cano | 202-502-8680

FERC Staff Report Identifies Lessons Learned From CIP Reliability Audits

Federal Energy Regulatory Commission (FERC) staff today issued a report offering recommendations to help users, owners, and operators of the bulk-power system assess their risk, compliance and overall cyber security. The findings in the report are based on lessons learned from several non-public audits of registered entities. These lessons learned can help facilitate compliance with mandatory reliability standards also, more generally, will facilitate efforts to improve the security of the nation's electric grid.

Staff from FERC's Office of Electric Reliability and Office of Enforcement conducted the audits in collaboration with staff from the North American Electric Reliability Corporation (NERC) and its regional entities. The audits assessed compliance with version 5 of NERC's Critical Infrastructure Protection (CIP) standards and also identified possible areas for improvement that are not specifically addressed by the CIP reliability standards. The audits were completed in fiscal years 2016 and 2017.

The report describes the lessons learned from the audits, including insights into the cyber security and CIP compliance issues encountered by the audited entities. These lessons learned will help other entities improve their compliance with the CIP reliability standards as well as their overall cyber security. Among staff's recommendations:

- 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;
- Ensure that policies and testing procedures for all electronic communications protocols are afforded the same rigor; and
- For each remote cyber asset conducting Interactive Remote Access, disable all other network access outside of the connection to the bulk electric system cyber system that is being remotely accessed, unless there is a documented business or operational need.

R-18-01

(30)