NEWS RELEASE

October 4, 2019

News Media Contact
Craig Cano | 202-502-8680

FERC Staff Report Highlights 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 improve their compliance with mandatory Critical Infrastructure Protection (CIP) standards as well as their overall cybersecurity posture.

The findings in the report are based on non-public CIP audits of registered entities that found most of the cybersecurity protection process and procedures adopted by the entities met the mandatory requirements of the standards. Staff said the lessons learned from the audits completed in fiscal year 2019 can help entities assess their risk and compliance with mandatory reliability standards and, more generally, can 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 and its regional entities. In addition to assessing compliance with the CIP reliability standards, the report includes recommendations regarding cybersecurity practices that are voluntary.

Among the report's recommendations:

- Consider all generation assets, regardless of ownership, when categorizing bulk electric system cyber systems associated with transmission facilities;
- Ensure that all employees and third-party contractors complete the required training and that the training records are properly maintained;
- Verify employees' recurring authorizations for using removable media; and
- Review all firewalls to ensure there are no obsolete or overly permissive firewall access control rules in use.

R-20-1

(30)