NEWS RELEASE

November 21,2019

News Media Contact

Craig Cano | 202-502-8680

Item No. A-4

FERC Staff Identifies Key Cybersecurity Program Priorities

The Federal Energy Regulatory Commission (FERC) staff today detailed the depth of its continuing efforts to address cybersecurity challenges facing the nation's energy infrastructure.

Among other things, the presentation detailed several organizational changes meant to better focus the agency's resources on quickly evolving cyber challenges including creation of a new security-focused group within the Office of Energy Projects' Division of Dam Safety and Inspections. The group will address cyber, as well as physical, security concerns at jurisdictional hydropower facilities, staff said in a presentation at FERC's November open meeting. Chairman Neil Chatterjee also announced that the Commission's Office of Electric Reliability would be realigning its functions to establish one division focused exclusively on cybersecurity.

"At FERC, we are charged with overseeing the development and enforcement of cybersecurity standards for the nation's high-voltage transmission system and jurisdictional hydroelectric facilities," FERC Chairman Neil Chatterjee said. "These two developments will help FERC staff more efficiently focus its efforts on cyber security. This new security group in OEP and the realignment in OER will consolidate the cybersecurity staff into a division that focuses solely on cyber."

Drawing on the experience and knowledge of each of the relevant offices, a FERC staff presentation today identified five areas where Commission staff will strategically and collectively focus efforts to address critical cybersecurity challenges. The five focus areas are:

- Supply Chain/Insider Threat/Third-Party Authorized Access;
- Industry access to timely information on threats and vulnerabilities;
- Cloud/Managed Security Service Providers;
- Adequacy of security controls; and
- Internal network monitoring and detection.

Staff also described certain outreach activities and other initiatives they intent to prioritize throughout FY2020. In particular, staff will closely monitor supply chain security implementation and the industry's adoption of new technologies and services to address cyber infrastructure implementation, maintenance and/or management. In addition, the Office of Energy Infrastructure Security continues to build on its existing outreach initiatives, including offering voluntary network architecture assessments and the Office of Electric Reliability will continue to conduct and participate in audits.

R-20-05

(30)