1977-2017
CELEBRATING 40 YEARS
Federal Energy Regulatory Commission

NEWS RELEASE

December 21, 2017

News Media Contact
Craig Cano | 202-502-8680

Docket Nos. RM18-2-000, AD17-9-000
Item No. E-1

FERC Proposes to Require Expanded Cyber Security Incident Reporting

The Federal Energy Regulatory Commission (FERC) today proposed development of a revised Critical Infrastructure Protection (CIP) Reliability Standard to improve mandatory reporting of cyber security incidents, including incidents that might facilitate future attempts to harm reliable operation of the nation's bulk electric system. A revised standard would enhance awareness of existing or developing threats.

"Cyber security is critical to protecting the nation's energy infrastructure, and we need to be vigilant and proactive in doing so," FERC Chairman Kevin J. McIntyre said. "To that end, this proposal is an important part of improving our awareness of existing as well as future cyber security threats and potential vulnerabilities."

Under the current CIP Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning), incidents must be reported only if they have compromised or disrupted one or more reliability tasks. FERC is concerned this threshold may understate the true scope of cyber-related threats facing the grid. In particular, the lack of any reported incidents in 2015 and 2016 suggests a gap in the current mandatory reporting requirement. The 2017 State of Reliability report by the North American Electric Reliability Corp. (NERC), which is responsible for enforcing FERC-approved mandatory reliability standards, echoed this concern.

Today's Notice of Proposed Rulemaking (NOPR) would direct NERC to submit modifications to broaden the requirement to include mandatory reporting of cyber security incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems (EACMS). In addition, the proposal would require NERC to modify the CIP Reliability Standards to:

- Specify the required information in cyber security incident reports to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; and
- Establish a deadline for filing a report once a compromise or disruption, or an attempted compromise or disruption, is identified by a responsible entity.

The NOPR would require that incident reports continue to go to the Electricity Information Sharing and Analysis Center (E-ISAC), but also would require that the reports be sent to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and that NERC file an annual, public and anonymized summary of the reports with FERC.

Comments on the NOPR are due 60 days after publication in the *Federal Register*.

R-18-06

(30)