NEWS RELEASE

July 19, 2018

News Media Contact

Craig Cano | 202-502-8680

Docket Nos. RM18-2-000

Item No. E-1

FERC Requires Expanded Cyber Security Incident Reporting

The Federal Energy Regulatory Commission (FERC) today directed the North American Electric Reliability Corp. (NERC) to develop, within six-months of the effective date of this final rule, modifications to the Critical Infrastructure Protection Reliability Standards to improve mandatory reporting of cyber security incidents, including attempts that might facilitate subsequent efforts to harm reliable operation of the nation's bulk electric system.

Under the current Critical Infrastructure Protection 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.

"Cyber threats to the bulk power system are ever changing, and they are a matter that commands constant vigilance," FERC Chairman Kevin J. McIntyre said. "Industry must be alert to developing and emerging threats, and a modified standard will improve awareness of existing and future cyber security threats."

Today's final rule directs NERC to modify the Standard to expand the current reporting requirement, including:

- Responsible entities must report cyber security incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS);
- Cyber security incident reports should be standardized to improve the quality of reporting and allow for ease of comparison across reports, analysis, and trending;
- Cyber security incident reports would be sent to those organizations best equipped to assess threats and communicate them to industry. Specifically, reports will continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC); the reports would also be sent to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). NERC would file an annual, public and anonymized summary of the reports with the Commission.

The Commission directed NERC to consider the threat level when developing reporting thresholds and timelines. Specifically the Commission directed NERC to consider the function of the EACMS and the nature of the attempted compromise or successful intrusion when developing the reporting thresholds so that only cyber security incidents meeting a certain threat level would have to be reported.

NERC also must develop reporting timelines that correspond to the adverse or attempted adverse impact to the grid that loss, compromise or misuse of the bulk electric system cyber assets could have on reliable operation. Prioritizing incident reporting will allow responsible entities to devote resources to reporting the most significant cyber security incidents faster than less significant events.

The Final Rule takes effect 60 days after publication in the *Federal Register*.

R-18-21 (30)