NEWS RELEASE

June 20, 2019

News Media Contact
Craig Cano | 202-502-8680

Docket No. RD19-3-000

FERC Strengthens Cyber Security Standards for Bulk Electric System

The Federal Energy Regulatory Commission (FERC) today bolstered the cyber security of the nation's bulk electric system by expanding the reporting requirements for incidents involving attempts to compromise operation of the grid. The action closes a gap in the prior Critical Infrastructure Protection Reliability Standards that required entities to report only when an incident has compromised or disrupted one or more reliability tasks.

FERC previously directed the North American Electric Reliability Corp. (NERC) to enhance the reporting of cyber security incidents out of concern that the existing standards may understate the true scope of threats by excluding from reporting incidents that could facilitate subsequent efforts to harm the reliable operation of the grid.

"Defending our nation's electric grid against cyber security threats is one of the Commission's most pressing challenges," Chairman Neil Chatterjee said. "It is vital that we ensure that NERC and the Department of Homeland Security have all the information needed to understand the evolving threat landscape for industrial control systems."

The approved new Critical Infrastructure Protection Reliability Standard CIP-008-6 (Cyber Security – Incident Reporting and Response Planning) now requires reporting of cyber security incidents that either compromise or attempt to compromise Electronic Security Perimeters, Electronic Access Control or Monitoring Systems, and Physical Security Perimeters associated cyber systems. The new Reliability Standard also encompasses disruptions or attempts to disrupt the operation of a bulk electric system cyber system.

Each responsible entity will be required to develop criteria for identifying an attempt to compromise a cyber asset and then apply those criteria during its cyber security incident identification process. This approach provides responsible entities the flexibility to develop criteria appropriate to their systems.

The revised standard also addresses the information to be included in Cyber Security Incident reports, their dissemination, and deadlines for filing. Reports and updates will be sent to the Electricity Information Sharing and Analysis Center and the Department of Homeland Security's National Cybersecurity and Communications Integration Center.

R-19-30

(30)