July 21, 2016

News Media Contact
Mary O'Driscoll | 202-502-8680

Docket Nos. RM15-14-002 and RM16-18-000
Item Nos. E-8 and E-10

FERC Directs Development of Standards for Supply Chain Cyber Controls

The Federal Energy Regulatory Commission (FERC) acted today to improve the cyber security of the bulk electric system by directing the North American Electric Reliability Corporation (NERC) to develop a new supply chain risk management standard that addresses risks to information systems and related bulk electric system assets.

In today's rule, FERC directed NERC to develop a forward-looking, objective-based Critical Infrastructure Protection (CIP) Reliability Standard that requires each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.

The new or modified Reliability Standard should address software integrity and authenticity; vendor remote access; information system planning; and vendor risk management and procurement controls. There is no requirement for any specific controls, nor does FERC require any "one-size-fits-all" requirements. The new or modified Reliability Standard should instead require responsible entities to develop a plan to meet the four objectives while providing flexibility to responsible entities as to how to meet those objectives. NERC is required to submit the new or modified Reliability Standard within one year of the effective date of the final rule.

The final rule will take effect 60 days after publication in the *Federal Register*.

Also today, FERC issued a Notice of Inquiry (NOI) into modifying CIP standards regarding the protection of control centers that are used to monitor and control the bulk electric system in real-time. Cyber systems are used extensively to operate and maintain interconnected transmission networks. The 2015 cyberattack on the electric grid in Ukraine is an example of how cyber systems used to operate and maintain interconnected networks more efficiently can have the unintended effect of creating cyber vulnerabilities.

In this case, the Commission is seeking comment on possible modifications, and any potential impacts they may have on the operation of the Bulk-Power System, to address separation between the internet and the cyber systems in control centers that perform transmission operator functions, and computer administration practices that prevent unauthorized programs from running, known as "application whitelisting," for cyber systems in control centers.

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

R-16-21

(30)