NEWS RELEASE

October 18, 2018

News Media Contact

Mary O'Driscoll | 202-502-8680

Docket Nos. RM17-13-000, R18-9-000

FERC Acts on Cyber Security Risks with New Supply Chain-Related Reliability Standards

The Federal Energy Regulatory Commission (FERC) today approved new mandatory Reliability Standards to bolster supply chain risk management protections for the nation's bulk electric system.

The new standards will augment current Critical Infrastructure Protection standards to mitigate cyber security risks associated with the supply chain for grid-related cyber systems.

Today's final rule closely follows what FERC outlined in the Notice of Proposed Rulemaking issued in January 2018.

The North American Electric Reliability Corporation (NERC) proposed the standards in response to FERC Order No. 829, which directed it to develop standards to address supply chain risk management for industrial control system hardware, software, and computing and networking services. The Commission notes that while the global supply chain provides opportunity for significant benefits to customers, it also presents opportunities to affect management or operations of generation or transmission companies that may result in risks to end-users.

In today's final rule, FERC said NERC's supply chain risk management Reliability Standards are forward-looking and objective-based, requiring 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 Commission also approved NERC's request for an 18-month implementation period, saying it was justified because longer time-horizon capital budgets and planning cycles may be necessary for the technical upgrades to meet the Reliability Standards' security objectives.

The Commission noted, however, that a significant cyber security risk remains because the standards exclude Electronic Access Control and Monitoring Systems (EACMS). EACMS include firewalls, authentication servers, security event monitoring systems, intrusion detection systems and alerting systems. They control electronic access into Electronic Security Perimeters and help protect high and medium impact bulk electric system (BES) cyber systems. Once an EACMS is compromised, an attacker could more easily control the BES cyber system or protected cyber asset.

To address that gap, FERC gave NERC 24 months to develop modifications that will include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.

Today's final rule takes effect 60 days after publication in the *Federal Register*.

Also today, FERC approved the 2019 business plan and budget for NERC, its regional entities and the Western Interconnection Regional Advisory Body.

R-19-02 (30)