NEWS RELEASES

FERC Proposes Incentives for Cybersecurity Investments by Public Utilities

December 17, 2020

Docket No. RM21-3-000
Item E-2: Staff Presentation | NOPR

The Federal Energy Regulatory Commission (FERC) took a major step toward enhancing the cybersecurity posture of the bulk power system today with a proposal for public utilities to secure incentive-based rate treatment for voluntary cybersecurity investments that go above and beyond mandatory Critical Infrastructure Protection (CIP) Reliability Standards.

Today's Notice of Proposed Rulemaking (NOPR) recognizes that the energy sector faces numerous and complex cybersecurity challenges at a time of both great change in the operation of the transmission system and an increase in the number and nature of attack methods. These ever-expanding risks create challenges in defending the digitally interconnected components of the grid from cyber exploitation.

In a June 2020 white paper, Commission staff sought comment on an incentive-based framework that could encourage public utilities to adopt best practices to protect their own transmission systems and improve the security of the

grid. Such a framework would allow the electric industry to be more agile in monitoring and responding to new and evolving cybersecurity threats, to identify and respond to a wider range of threats, and to address threats with comprehensive and more effective solutions.

The proposed rule would allow public utilities to seek Commission approval, pursuant to section 205 of the Federal Power Act, of two types of incentives for cybersecurity investments: a rate of return (ROE) adder of 200 basis points or deferred cost recovery for certain cybersecurity-related expenses. Qualifying expenditures would be eligible for either, but not both, incentives. The total cybersecurity incentives requested would be capped at the zone of reasonableness.

The incentives would be available for certain investments that voluntarily apply specific CIP Reliability Standards to facilities that are not subject to those requirements and/or implement standards and guidelines from the National Institute of Standards and Technology's (NIST) voluntary Framework for Improving Critical Infrastructure Cybersecurity.

Deferred cost recovery would be allowed for three categories of expenses: expenses associated with third-party provision of hardware, software and computing networking services; expenses for training to implement new cybersecurity enhancements undertaken pursuant to this rule; and other implementation expenses, such as risk assessments by third parties or internal system reviews and initial responses to findings of such assessments. Prior or continuing costs would not be eligible for incentives; deferred regulatory assets whose costs are typically expensed would be amortized over a five-year period.

Public utilities seeking to implement the proposed incentives must obtain prior Commission approval, and the proposed rule would impose initial and annual reporting requirements.

Comments on the NOPR are due 60 days after publication in the *Federal Register*, with reply comments due 30 days later.

R-21-9