BRACEWELL

INSIGHTS

FERC Proposes Incentive-Based Rate Treatment for Cybersecurity Investments

December 22, 2020

By: ***Catherine P. McCarthy*** ***Joshua Robichaud***

On Thursday, December 17, 2020, the Federal Energy Regulatory Commission ("FERC") issued a ***Notice of Proposed Rulemaking*** ("NOPR" or "Proposed Rule") seeking comment on proposals that would allow public utilities to make a filing pursuant to Section 205 of the Federal Power Act ("FPA") to seek incentive-based rate treatment for certain cybersecurity investments made to improve the security of the Bulk-Power System ("BPS").***[1]*** The NOPR follows a white paper published by FERC staff in June 2020, which expressed concern that the promulgation of mandatory reliability standards in accordance with Section 215 of the FPA may not be effective in responding to complex and rapidly evolving cybersecurity threats, and solicited comments on whether the Commission should use its ratemaking authority to encourage utilities to undertake additional investments on a voluntary basis.

Consistent with this approach, the NOPR proposes to provide public utilities with the option to seek certain rate incentives, including a return on equity ("ROE") adder and deferred cost recovery, for voluntary cybersecurity investments in BPS facilities as well as informational and operational technology networks used to provide FERC-jurisdictional services. Possible incentives include the opportunity to seek a Return on Equity ("ROE") adder of 200 basis points, subject to a cap at the upper end of the utility's ROE zone of reasonableness, and the opportunity to establish a regulatory asset for expenses for activities that exceed the CIP Reliability Standards to defer recovery of such costs by amortizing recovery over a five year period and including the utility asset in transmission rate base. Although much of the discussion in the NOPR focuses on encouraging investments by transmission-owning utilities, the NOPR suggests that FERC may be open to providing generation owners and developers to seek incentives in certain circumstances.

The NOPR comes at a time when the federal government is moving aggressively to mitigate perceived cybersecurity threats to critical infrastructure. Notably, on the same day that FERC issued the NOPR, the Secretary of Energy issued an order***[2]*** prohibiting certain electric utilities from installing equipment, components, or software manufactured or controlled by Chinese companies in furtherance of the objectives set out in President Trump's May 1, 2020 Executive Order on securing the BPS.***[3]*** These issues have become only more salient in recent weeks following the revelation that SolarWinds, a major IT service provider for federal agencies and electric power utilities, was ***hacked***, and some media sources indicated that FERC itself was subject to "***highly malicious activity***."***[4]***

The following sections provide an overview of the framework set out in the NOPR. Comments on the NOPR are due 60 days after the NOPR's publication in the Federal Register, and reply comments are due 30 days later.

Background and Overview

The Proposed Rule largely follows the framework outlined in the white paper and is intended to incent public utilities to undertake voluntary cybersecurity investments above and beyond those outlined in the mandatory Critical Infrastructure Protection ("CIP") Reliability Standards. Notably, while FERC has authority to grant transmission incentives pursuant to Section 219 of the FPA, the NOPR acknowledges that FERC has decided not to rely on its Section 219 authority in order to encompass a broader array of assets and investments that have the potential to contribute to grid security. Instead, relying on Sections 205 and 206 of the FPA, FERC proposes to modify its regulations to establish rules for incentive-based treatment for voluntary cybersecurity investments made "by a public utility for or in connection with the transmission or sale of electric energy subject to the jurisdiction of the Commission."***[5]*** Thus, FERC explains that it is proposing to provide "incentives for cybersecurity investment not only in transmission facilities but also for cybersecurity investment in information technology and operational technology networks that a public utility uses to provide other jurisdictional services."***[6]***

FERC's reference to investments in technology and networks used to provide other jurisdictional services appears broad enough to encompass investment by an array of entities that play a role in maintaining the security and reliability of the grid, such as owners and operations of generation facilities. It is important to note, however, that the NOPR does not provide any guidance regarding whether FERC would be open to considering requests for incentive rate treatment from entities other than transmission-owning utilities and, if so, what form such recovery would take. FERC has recognized in principle that generation owners and operators should be permitted to recover prudently incurred costs associated with compliance with Reliability Standards. For instance, FERC previously has stated that it will permit "recovery of all costs prudently incurred to comply with the Reliability Standards"***[7]*** and recently approved a proposal by ISO New England Inc. to permit the owners of generation and transmission facilities critical to the derivation of system operating limits to recover costs associated with the compliance with CIP Reliability Standards.***[8]*** Given that owners of certain generation facilities provide services critical to the reliability of the transmission grid, such as black start service and reactive power, voluntary investments made by these entities to improve the reliability of the BPS could potentially qualify for treatment similar to the treatment afforded to investments made by transmission owners. Generation owners that are interested in seeking recovery of voluntary investments in cybersecurity capabilities could comment on the NOPR requesting guidance from FERC regarding incentive requests by non-transmission owners.

Eligibility for Incentives

The NOPR proposes to allow public utilities to receive incentive rate treatment for investments falling into two categories:

- Voluntary application of North American Electric Reliability Corporation ("NERC") CIP Reliability Standards to facilities that are not currently subject to those requirements; and

- Implementation of security controls included in the U.S. Department of Commerce, National Institute of Standards and Technology's ("NIST") Framework for Improving Critical Infrastructure Cybersecurity ("NIST Framework") to encourage the deployment of automated and continuous monitoring controls to enhance data collection and security awareness.

Each of these approaches is outlined in further detail below.

NERC CIP Incentives Approach

The NERC CIP Incentives Approach allows a public utility to seek to receive incentive rate treatment for voluntarily applying identified CIP Reliability Standards to facilities that are not currently subject to those requirements. By way of background, the CIP Reliability Standards utilize a tiered structure that classifies assets into three types of systems:

- High impact systems are critical cyber linkages in the grid system, including large control centers.

- Medium impact systems are a tier below and include smaller control centers, ultra-high voltage transmission, and large substations and generating facilities.

- Low impact systems are assets not designated as high or medium impact systems.
  As a general matter, the most complex and costly requirements are imposed on high impact systems, given their system, with less onerous standards and requirements applied to medium and low impact systems.
  In light of this framework, the NOPR identifies two scenarios in which FERC may authorize such incentives:

- *Med/High*: A utility can receive incentive rate treatment for voluntarily applying a higher classified system's requirements to a lower classified system (*e.g.*, applying a high impact standard to a medium impact system or a high or medium impact standard to a low impact system). In doing so, a public utility can choose to apply the higher standard to some or all of its lower impact system but would receive incentive rate treatment only for the incremental investments it makes to apply the more stringent protections.

- *Hub-Spoke*: A public utility can receive incentive rate treatment for voluntarily ensuring that all external routable connectivity to and from the low impact system connects to a high or medium impact system. The public utility must also apply the cyber communications security controls from the high or medium impact system to the connected low impact system. The lower impact system inherits the additional protections provided by the higher impact system's compliance with its relevant CIP Reliability Standards through this methodology.

NIST Framework Approach

This approach allows a public utility to seek to receive incentive rate treatment for adopting certain security controls included in the NIST Framework that go above and beyond the requirements of the CIP Reliability Standards. FERC explains that while the NIST Framework sets out standards, guidelines, and best practices respecting an array of security controls, FERC is proposing to limit initial eligibility for cybersecurity incentives to the use of automated and

continuous monitoring controls most likely to provide a benefit to the cybersecurity of FERC-jurisdictional transmission facilities (rather than the broader bulk electric system). This could include, for instance, installation of a dynamic asset management program that automatically scans hardware and software for evidence of unauthorized access or implementation of a "sandbox" to identify and isolate malicious code and malware. FERC indicates that it anticipates that the types of security controls eligible for incentives will need to evolve over time in response to changes in cybersecurity risks.

Available Incentives

ROE Adder Incentive

A public utility can request an ROE adder of 200 basis points for cybersecurity investments deemed eligible under either the NERC CIP Incentives Approach or the NIST Framework Approach. The ROE incentive is intended to encourage proactive investment in cybersecurity systems but is limited to capital investments. Eligible capital investments can take the form of transmission-specific investments or enterprise-wide costs, if such enterprise-wide costs are recovered through transmission rates, and the public utility can demonstrate how the investment will materially enhance the security posture of the BPS. The Commission expects the dollar amounts associated with these investments to be limited and therefore should not significantly impact rates. Furthermore, the total cybersecurity incentives requested for a particular investment would be capped at the upper end of the public utility's zone of reasonableness. FERC's transmission ROE policies have been in flux for almost a decade but most recently, the method applied by FERC has resulted in more narrow zones of reasonableness than resulted from past ROE methods. It is possible, therefore, that some transmission owner ROE "upside" from obtaining a 200 basis point ROE adder could evaporate as a result of being capped at the upper end of the zone or reasonableness. FERC has not considered a utility's ROE on all transmission investments in capping ROE in the context of transmission incentives and has instead done so on a project-by-project basis.

Regulatory Asset Incentive

A public utility may seek to defer recovery of certain cybersecurity costs that are generally expensed as incurred, and treat them as regulatory assets, while also allowing such regulatory assets to be included in transmission rate base. Furthermore, such deferred regulatory assets whose costs are typically expensed should be amortized over a five-year period and, during that period, included as transmission rate base. As with the ROE Adder Incentive, only expenses for activities that exceed the CIP Reliability Standards are eligible. Furthermore, expenses that are mandatory, incurred on a regular or ongoing basis, or are incurred prior to the request for incentive rate treatment are ineligible for the Regulatory Asset Incentive. FERC also proposes that only directly assigned transmission costs or the allocated portion of enterprise-wide expenses could qualify for this incentive. Therefore, deferred cost recovery and treatment of such costs as a regulatory asset to be included in transmission rate base will be permitted for three types of expenses: 1) third-party provision of hardware, software, and computing networking services; 2) training to implement new cybersecurity enhancements undertaken pursuant to this rule; and 3) other implementation expenses, such as system assessments by third parties or internal system reviews. FERC proposes that five years is a reasonable amount of time to earn a return on expenses that are not typically eligible for an ROE. FERC also notes

that five years is also consistent with the typical lifespan and depreciation of cybersecurity investments.

Other Types of Incentives

In addition to the incentives outlined above, the Proposed Rule includes a provision allowing the Commission flexibility to grant a public utility other incentives that it deems just and reasonable and not unduly discriminatory or preferential for investments undertaken pursuant to this rule. Such additional forms of incentives will be considered on a case-by-case basis.

Application Procedure and Rate Recovery

In order to benefit from the incentives set out above, a public utility is required to make a Section 205 filing with FERC requesting incentive rate treatment. Applicants requesting incentives on the basis that the utility had extended the application of the CIP Reliability Standards in accordance with the Med/High or Hub-Spoke approaches described above would be entitled to a rebuttable presumption that the investments enhance the BPS's security posture. Public utilities requesting incentives for implementation of NIST Framework requirements would not be entitled to a rebuttable presumption, but would be required to demonstrate that the investment materially enhances the cybersecurity posture of the BPS.

In the centralized markets context, the ISO or RTO may seek to modify its tariff to incorporate transmission owners' incremental revenue requirements resulting from these incentives and to allocate those costs to transmission customers. The ISO and RTO construct could also incorporate a mechanism for generation owners currently selling under market-based rates to recover cost-based revenue requirements related to the proposed incentives and to allocate those costs to transmission customers. Transmission owners with a formula rate may need to tweak the formula rate as part of the Section 205 filing to reflect rate recovery for the incentives whether within or outside the ISO and RTO context. Also, transmission owners with a fixed stated rate outside the ISO or RTO context may need to file a single issue rate case, possibly as part of the Section 205 submittal, possibly proposing a rider or surcharge to its existing rate to modify the rate to incorporate the ROE adder or new regulatory asset.

If an incentive request were approved, a public utility would be eligible to receive the incentive for the lesser of 1) the depreciation life of the underlying asset, 2) 10 years from when the cybersecurity improvements enter service, 3) when the investments or activities that serve as the basis of that incentive become mandatory pursuant to a Reliability Standard approved by the Commission, or 4) when the public utility no longer meets the requirements for receiving the incentive. Any public utility receiving incentives would be required to notify the Commission within 120 days of the completion of the relevant cybersecurity improvement and to submit an informational filing on an annual basis substantiating the nature of the investment and the associated ratemaking treatment.

The NOPR explains that public utilities that received incentives would not be penalized by FERC for failing to voluntarily follow a proposed standard or requirement. However, public utilities would be prohibited from receiving the incentive for the period during which it fails to comply with the relevant standard. FERC also explains that it would revoke any incentives if it determined that the public utility met applicable requirements as a result of an FPA Section 206 proceeding initiated by the Commission or a third party.

[1] *Cybersecurity Incentives*, Docket No. RM21-3-000, 173 FERC ¶ 61,240 (2020) ("NOPR").

[2] Dept. of Energy, Prohibition Order Securing Critical Defense Facilities (Dec. 17, 2020).

[3] Executive Order 13920, Executive Order on Securing the United States Bulk-Power System (Issued May 1, 2020).

[4] Blake Scobzak, *Major Hack Hits Energy Companies, U.S. Agencies*, E&E News (December 15, 2020); Natasha Bertrand and Eric Wolff, *Nuclear Weapons Agency Breached Amid Massive Cyber Onslaught*, Politico, (December 17, 2020).

[5] NOPR at P 20.

[6] *Id.*

[7] *Rules Concerning the Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs ¶ 31,204 at P 259 (2006).

[8] *ISO New England Inc.*, 171 FERC ¶ 61,160 (2020).