HEADLINES

Staff Presentation on Cybersecurity Incentives (RM21-3-000)

December 17, 2020

Staff Presentation: December 17, 2020
Docket No. RM21-3-000
Item E-2: NOPR | News Release

Good morning, Chairman Danly and Commissioners

Item E-2 is a draft Notice of Proposed Rulemaking, or NOPR, pursuant to sections 205 and 206 of the Federal Power Act, that would allow public utilities to request incentives for certain cybersecurity investments that go above and beyond the requirements of the North American Electric Reliability Corporation, or NERC, Critical Infrastructure Protection Reliability Standards, the CIP Reliability Standards.

The proposed cybersecurity incentives framework encourages public utilities to undertake cybersecurity investments on a voluntary basis that are above and beyond the requirements of the mandatory CIP Reliability Standards and, thereby, better ensure secure service for ratepayers. This approach would incent a public utility to adopt cybersecurity practices that would not only better protect its own systems but also improve the cybersecurity of the Bulk-Power System.

The draft NOPR includes two incentive approaches:

The first approach, the NERC CIP Incentives Approach, would allow a public utility to receive incentive rate treatment for voluntarily applying identified CIP Reliability Standards to facilities that are not currently subject to those requirements.

- Under the NERC CIP Incentives Approach, a public utility has two options for requesting an incentive. A public utility would request incentive rate treatment for voluntarily applying the requirements for medium or high impact systems to low impact systems, and/or the requirements for high impact systems to medium impact systems, referred to as the Medium/High Incentive.
- Alternatively, or in addition to the Medium/High Incentive, a public utility would request incentive rate treatment for voluntarily ensuring that all external routable connectivity to and from the low impact system connect to a high or medium impact bulk electric system Cyber System, referred to as the Hub-Spoke Incentive.

The second approach would allow a public utility to receive incentive rate treatment for implementing certain security controls included in the Cybersecurity Framework developed by the National Institute of Standards and Technology, the NIST Framework. This is the NIST Framework Approach.

The NIST Framework includes many types of security controls; however, the draft NOPR proposes to initially only consider one type of security controls, automated and continuous monitoring, as eligible for an incentive under this approach.

The draft NOPR would allow a public utility to request incentives using any combination of the two proposed approaches.

Under the draft NOPR, a public utility that makes cybersecurity investments consistent with the two approaches that we have described would be eligible for one of the following two types of incentives:

The first incentive would apply a 200 basis-point adder to the return on equity for eligible cybersecurity capital investments and is referred to as the Cybersecurity ROE Incentive.

Alternatively, the second incentive would allow a public utility to seek deferred cost recovery for certain expenses related to cybersecurity investments and is referred to as the Regulatory Asset Incentive.

Finally, the draft NOPR describes the showings that a public utility would have to make to receive either incentive and would require an annual informational filing.

Initial comments are due 60 days, and reply comments 90 days, after the date of publication in the Federal Register.

Thank you, this concludes our presentation. We would be happy to address any questions.