

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Cybersecurity Incentives

)

Docket No. RM21-3-000

**COMMENTS OF
THE INDUSTRIAL ENERGY CONSUMERS OF AMERICA**

April 6, 2021

TABLE OF CONTENTS

I. BACKGROUND 2

II. COMMENTS 4

1. The Commission should not pre-empt NERC and the responsibilities that Congress has given to NERC for reliability. Instead of adopting new rules, the Commission should direct NERC to review its CIP reliability standards to determine whether new standards are needed rather than preemptively increasing consumers’ costs..... 4

2. The Commission has not established a record that voluntary cybersecurity investments are needed or that utilities need additional incentives to make those investments..... 5

3. The Commission should not incentivize utilities to comply with two sets of reliability standards..... 6

4. The Commission cannot circumvent the consumer protection aspects of FPA Section 219 by proposing to establish incentive-based rate treatment for cybersecurity investments under FPA Sections 205 and 206. The Commission should narrow the scope of any rules to provide cybersecurity incentives to the Commission’s authority under FPA Section 219. 6

5. If the Commission adopts cybersecurity incentives, the ROE incentive adder should not exceed 50 basis points..... 7

6. If the Commission adopts cybersecurity incentives, the incentives should have a sunset date of no more than three years..... 8

III. CONCLUSION..... 10

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Cybersecurity Incentives

)

Docket No. RM21-3-000

**COMMENTS OF
INDUSTRIAL ENERGY CONSUMERS OF AMERICA**

The Federal Energy Regulatory Commission (“Commission” or “FERC”) should reconsider its proposed rules to incentivize cybersecurity investments. The North American Electric Reliability Corporation (“NERC”) is the Commission-approved Electric Reliability Organization. The Commission should direct NERC to review its Critical Infrastructure Protection (“CIP”) reliability standards and consider updating the standards to include some of the investments identified in the Commission’s Notice of Proposed Rulemaking (“NOPR”), instead of adopting incentives under Sections 205 and 206 of the Federal Power Act (“FPA”). Further, if the Commission is determined to adopt incentive ratemaking treatment for cybersecurity investments, then it should do so under Section 219 of the FPA and, accordingly, ensure consumer protections to prevent excessive and unnecessary utility spending on such investments.

Industrial Energy Consumers of America (“IECA”)¹ welcomes the opportunity to submit these Comments on the FERC’s proposed rules regarding cybersecurity incentives for utilities.² As explained in these Comments, Congress gave NERC responsibility for grid reliability and setting mandatory cybersecurity standards. NERC has already established, and FERC has

¹ IECA is a nonpartisan association of leading manufacturing companies with \$1.0 trillion in annual sales, over 3,700 facilities nationwide, and with more than 1.7 million employees. IECA members represent a diverse set of industries including chemical, plastics, steel, iron ore, aluminum, paper, food processing, fertilizer, insulation, glass, industrial gases, pharmaceutical, building products, automotive, independent oil refining, and cement.

² *Combined Notice of Filing #1*, February 12, 2021; *Errata Notice Extending Comment Date*, February 12, 2021.

approved, mandatory CIP reliability standards for cybersecurity. If different or more stringent standards are necessary, then NERC should decide what standards to adopt and then seek Commission approval of the standards. IECA supports proper ratemaking that establishes just and reasonable rates while maintaining reliability. While IECA appreciates the Commission's interest in maintaining reliability through protection of utilities and the Bulk Electric System from cyber-attacks, the Commission need not adopt incentives to achieve those outcomes.

I. BACKGROUND

In its NOPR, the Commission proposed under Sections 205 and 206 of the FPA to establish rules for incentive-based rate treatment for voluntary cybersecurity investments by FERC-jurisdictional utilities.³ Voluntary cybersecurity investments refer to those cybersecurity investments that are not required to meet mandatory NERC CIP reliability standards. Accordingly, the Commission's proposed rules would provide cybersecurity incentives to public utilities that make certain cybersecurity investments that go above and beyond the requirements of NERC's CIP reliability standards. FERC asserts that its proposal would materially enhance the cybersecurity posture of utilities and the Bulk Electric System by enhancing utilities' cybersecurity posture to the benefit of ratepayers, despite the impact on rates.

The Commission states that its proposed rules are intended to establish a two-prong approach to cybersecurity – (1) mandatory NERC CIP reliability standards and (2) a cybersecurity incentives framework. While the Commission has already approved mandatory NERC CIP reliability standards, the Commission asserts that public utilities may not have the appropriate economic incentives to invest in cybersecurity measures that go above and beyond the mandatory NERC CIP reliability standards. The Commission asserts that its approach will benefit ratepayers

³ *Cybersecurity Incentives*, Notice of Proposed Rulemaking, Docket No. RM21-3-000 (issued December 7, 2020) (the "NOPR"), 86 Fed. Reg. 8309 (Feb. 5, 2021).

by incentivizing public utilities to use known, effective, and dynamic solutions to cybersecurity threats. The Commission argues that while its proposal will have an impact on rates, it believes that the impact to consumers will be outweighed by utilities having a more secure grid for the benefit of ratepayers. However, the Commission makes no assertion that its currently reliability framework is insufficient to protect the Bulk Electric System from cybersecurity attacks and makes no showing that incremental expenditures by utilities on cybersecurity measures will provide quantifiable commensurate benefits.

The Commission issued its proposed rules under FPA Sections 205 and 206. FPA Sections 205 and 206 are broader than Congress's directive to the Commission under FPA Section 219. Under FPA Section 219, Congress required the Commission to issue rules that would provide incentive rate treatment for the transmission of electric energy in interstate commerce by public utilities *for the purpose of benefitting consumers by ensuring reliability and reducing the cost of delivered power* by reducing transmission congestion.⁴ In its NOPR, the Commission attempts to avoid relying on Section 219, which has certain built-in consumer protections, and, instead, proposes its rules under FPA Sections 205 and 206. The Commission asserts that it is proposing its cybersecurity incentives under a different statute because the incentives are for a different purpose than other transmission-related rate incentives. The Commission avers that it intends to provide incentives not just for cybersecurity investments for transmission service, but also for information technology and operational technology networks that public utilities use to provide jurisdictional services other than transmission service.⁵

⁴ 51 U.S.C. 824s(a) (emphasis added).

⁵ NOPR at P. 22.

II. COMMENTS

The Commission should seek to protect consumers from excessive and unnecessary utility spending on voluntary cybersecurity investments.

- 1. The Commission should not pre-empt NERC and the responsibilities that Congress has given to NERC for reliability. Instead of adopting new rules, the Commission should direct NERC to review its CIP reliability standards to determine whether new standards are needed rather than preemptively increasing consumers' costs.**

The Energy Policy Act of 2005 added FPA Section 215, which requires a Commission-certified Electric Reliability Organization to develop mandatory and enforceable reliability standards, including requirements for cybersecurity protections which are subject to Commission review and approval. Accordingly, the Commission issued Order No. 672 implementing FPA Section 215 and certifying NERC as the Electric Reliability Organization.⁶ Pursuant to the process and roles set forth by Congress, NERC issues CIP Reliability Standards and the Commission approves them.⁷

The NERC CIP reliability standards are intended to constitute a defense-in-depth approach based on an assessment of risk. The Commission's Staff has noted that NERC's CIP reliability standards "are objective-based and allow responsible entities to choose compliance approaches best tailored to their systems."⁸ The NERC standards work and are designed to provide the same flexibility the Commission intends to promote through its rulemaking. Further, Version 5 of NERC's CIP reliability standards became enforceable for high and medium impact Cyber Systems

⁶ *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

⁷ See Order No. 706, 122 FERC ¶ 61,040 at P 1; *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

⁸ *Cybersecurity Incentives Policy White Paper*, Notice of White Paper, Docket AD20-19-000 (issued June 18, 2020) (White Paper).

on July 1, 2016, while the reliability standards for low impact Cyber Systems just recently became enforceable on April 1, 2020.⁹ Because it has been five years since the NERC CIP reliability standards became enforceable for high and medium impact systems, the Commission should direct NERC to review whether additional updates to the standards are necessary before considering whether to adopt a Final Rule that would provide incentives to potentially achieve the same outcomes.

Writing separately in the NOPR, Chairman Glick and Commissioner Danly request Comments on whether the Commission can better address cybersecurity threats by directing NERC to expand its CIP standards to require some, or all, of the investments contemplated in the NOPR. As set forth in these Comments, the answer to their question is – yes. The Commission can better address cybersecurity threats by directing NERC to consider expansion and evolution of its CIP reliability standards to align with the initiatives contemplated in the NOPR.

2. The Commission has not established a record that voluntary cybersecurity investments are needed or that utilities need additional incentives to make those investments.

The Commission has not established a record that voluntary cybersecurity investments are needed to protect utilities and Bulk-Electric System, or that incentives and the commensurate consumer burden are needed for utilities to make those investments. The Commission’s NOPR remains unreasonably vague about the scope of the cybersecurity threat to utilities and the Bulk-Electric System. The Commission has not demonstrated that utilities and the Bulk-Electric System are not already protected from cybersecurity threats through capital investments made by utilities to comply with the NERC CIP reliability standards. And, if utilities and the Bulk-Electric System are not adequately protected from cybersecurity threats, then the Commission has not

⁹ See Order No. 791, 145 FERC ¶ 61,160.

demonstrated that security cannot be provided or addressed by additional NERC CIP reliability standards. The Commission proposes to provide cybersecurity incentives to utilities on the backs of ratepayers without establishing a record that such incentives are needed or effective.

3. The Commission should not incentivize utilities to comply with two sets of reliability standards.

FERC should not incentivize utilities to comply with two sets of standards – NERC standards and National Institute of Standards and Technology (“NIST”) standards. If the existing NERC CIP reliability standards are inadequate, then NERC should consider updating its standards to integrate or adopt certain NIST standards, with Commission approval. Streamlined, consistent, and uniform cybersecurity standards should remain a priority. Introducing additional, non-NERC standards detracts from that priority and is inconsistent with the responsibilities that Congress granted to NERC.

4. The Commission cannot circumvent the consumer protection aspects of FPA Section 219 by proposing to establish incentive-based rate treatment for cybersecurity investments under FPA Sections 205 and 206. The Commission should narrow the scope of any rules to provide cybersecurity incentives to the Commission’s authority under FPA Section 219.

In 2005, in response to the Northeast blackout of 2003, Congress directed FERC to “establish, by rule, incentive-based (including performance-based) rate treatments for the transmission of electric energy in interstate commerce by public utilities for the purpose benefitting consumers by ensuring reliability and reducing the cost of delivered power by reducing transmission congestion.”¹⁰ With FPA Section 219, Congress directed FERC to establish incentive-based rate treatments (1) for the benefit of consumers and (2) to reduce the cost of delivered power.

¹⁰ 16 U.S.C. § 824s(a).

In this case, the Commission proposes a 200-basis point ROE adder for eligible cybersecurity investments, among other incentives. Electric transmission will comprise the overwhelming majority of the Commission-jurisdictional assets and activities that would qualify for the proposed ROE adder. For that reason, any incentives granted to transmission-owning utilities must be subject to FPA Section 219. The potential that certain other Commission-jurisdictional asset owners – such as generation owners that have cost-based rates on file with the Commission – are subject to cybersecurity requirements does not detract from the reality that FPA Section 219 applies to incentives granted to transmission-owning utilities. The requirements of FPA Section 219 do apply.

5. If the Commission adopts cybersecurity incentives, the ROE incentive adder should not exceed 50 basis points.

The Commission's proposed incentives for cybersecurity investments include: (1) an increase in the ROE of 200 basis points, (2) deferred cost recovery, or (3) any other incentives approved by the Commission, pursuant to the requirements of the rule, that are deemed to be just and reasonable and not unduly discriminatory or preferential. Whichever incentive is approved by the Commission for a particular utility's investment, the ultimate cost will be paid by consumers. If the Commission adopts incentive ratemaking for cybersecurity investments, and the benefits of any discretionary investment are shown to exceed the costs associated with the investment, then such incentive should not exceed a 50 basis point ROE incentive adder. The 200-basis point ROE incentive is excessive and much higher than other project-specific ROE incentives that currently exist and should be lowered to a level that presents a lesser burden on consumers.

6. If the Commission adopts cybersecurity incentives, the incentives should have a sunset date of no more than three years.

In the Staff White Paper, the Commission's Staff proposed that "incentivized cybersecurity investments should have a sunset date of no more than three to five years."¹¹ But instead of adopting a three-to-five-year sunset date as recommended by the Commission's Staff, the Commission proposes to allow utilities to receive cybersecurity incentives 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/activities serving as the basis for the incentive become mandatory; or (4) when the public utility no longer meets the requirements for receiving the incentive. While limiting the incentives to the lesser eventuality provides some protection for consumers, the Commission's proposal for some incentives to last 10 years from when they are placed in service is far too long.

No cybersecurity incentive should last for more than three years from when the investment is made. The three-year sunset date would provide an incentive for utilities to make cybersecurity investments in NERC CIP reliability standards after they have been developed and approved but before they become fully implemented and enforceable. The three-year sunset date would be a short-term incentive for the purpose of expediting investment to comply with NERC CIP reliability standards while the standards are in the process of becoming fully implemented and enforceable. NERC CIP reliability standards should not take five years to be implemented, so neither should cybersecurity incentives last for five years. And even if NERC CIP reliability standards do take longer than five years to be developed and implemented, those utilities that make the cybersecurity investments early still receive the benefits of a three-year incentive and a more secure system.

¹¹ *Cybersecurity Incentives Policy White Paper*, Notice of White Paper, Docket AD20-19-000 (issued June 18, 2020) (White Paper) at Pg. 23.

The three-year sunset date would also protect consumers from paying for obsolete investments. As noted by the Commission's Staff, there are significant differences between cybersecurity investments and other incentives that the Commission has granted.¹² Because of the rapidly changing cybersecurity environment and rapid advances in technology, cybersecurity investments can become obsolete or provide significantly reduced value in a comparatively short period of time. It would be unjust and unreasonable for consumers to pay cybersecurity incentives for investments that have become obsolete and are no longer useful. To protect consumers from continuing to pay incentives long after the investments have become obsolete, the Commission should find that any incentives associated with discretionary cybersecurity investments should have a sunset date of no more than three years.

¹² *Id.*

III. CONCLUSION

WHEREFORE, Industrial Energy Consumers of America respectfully request that the Commission afford due consideration to these Comments.

Respectfully submitted,

McNEES WALLACE & NURICK LLC

By: */s/ Robert A. Weishaar, Jr.*

Robert A. Weishaar, Jr.
1200 G Street NW, Suite 800
Washington, DC 20005
Phone: (202) 898-5700
Fax: (717) 260-1765
Email: bweishaar@mcneeslaw.com

Bryce A. McKenney
21 East State Street, 17TH Floor
Columbus, OH 43215
Phone: (614) 719-2842
Fax: (614) 469-4653
Email: bmckenney@mcneeslaw.com

Counsel to Industrial Energy Consumers of America

Dated: April 6, 2021

CERTIFICATE OF SERVICE

I hereby certify that I have this day served, via first-class mail, electronic transmission, or hand-delivery the foregoing upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, DC this 6th day of April, 2021.

/s/ Robert A. Weishaar, Jr.

Robert A. Weishaar, Jr.
McNees Wallace & Nurick LLC
1200 G Street, NW, Suite 800
Washington, DC 20005
Phone: (202) 898-5700
Fax: (717) 260-1765
Email: bweishaar@mcneeslaw.com

Counsel to Industrial Energy Consumers of
America