UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives	**)**	
Policy White Paper	**)**	**Docket No. AD20-19-000**

COMMENTS OF WIRES

WIRES, on behalf of its members, respectfully submits the following Comments on the Notice of White Paper ("White Paper") issued by the Federal Energy Regulatory Commission ("Commission" or "FERC") on June 18, 2020.[1] As the Commission explained, the White Paper's purpose is to explore "a new framework for providing transmission incentives to utilities for cybersecurity investments that produce significant cybersecurity benefits for actions taken that exceed the requirements of the Critical Infrastructure Protection Reliability Standards (CIP Reliability Standards).[2]

WIRES is an international non-profit trade association of investor-, publicly- and cooperatively-owned transmission providers and developers, transmission customers, regional grid managers, and equipment service companies.[3] WIRES promotes investment in electric transmission and state and federal policies that advance energy markets, economic efficiency, a more resilient grid, and consumer and environmental benefits through development of electric transmission infrastructure. WIRES strongly supports the Commission's efforts to incentivize cybersecurity investments in order to promote a more reliable and resilient grid, and submits the following comments for consideration.

---

[1] Federal Energy Regulatory Commission, Cybersecurity Incentives Policy White Paper (June 2020).
[2] White Paper at 3.
[3] This filing is supported by the full supporting members of WIRES but does not necessarily reflect the views of the Regional Transmission Operator/Independent System Operator ("RTO/ISO") associate members of WIRES. For more information about WIRES, please visit www.wiresgroup.com.

I. COMMUNICATIONS

In accordance with Rule 203(b)(3) of the Commission's Rules of Practice and Procedure, all communications regarding these comments should be directed to:

Larry Gasteiger
Executive Director
WIRES
1325 G Street, N.W., Suite 500
Washington, DC 20005
Office: (202) 449-7673
Cellphone: (703) 980-5750
lgasteiger@exec.wiresgroup.com

II. COMMENTS

A. The Commission Should Not Let Its Work On Cybersecurity Incentives Delay Completion Of A Final Transmission Incentives Rule.

On March 20, 2020, the Commission issued a Notice of Proposed Rulemaking proposing to revise its existing transmission incentives policy and corresponding regulations promulgated in Order No. 679[4] pursuant to section 219 of the Federal Power Act ("FPA")[5] in light of changes in transmission development and planning in recent years.[6] Although the Incentives NOPR proposed various incentives for transmission projects, including projects that provide reliability benefits, the Commission carved out cybersecurity incentives to be addressed "independently in a separate, future proceeding."[7]

WIRES filed initial and reply comments strongly supporting the Commission's efforts to adopt and implement transmission rate incentives policies designed to promote and incentivize

[4] *Promoting Transmission Investment through Pricing Reform*, Order No. 679, 116 FERC ¶ 61,057, *order on reh'g*, Order No. 679-A, 117 FERC ¶ 61,345 (2006), *order on reh'g*, 119 FERC ¶ 61,062 (2007).
[5] 16 U.S.C. § 824s.
[6] *Elec. Transmission Incentives Policy Under Section 219 of the Fed Power Act*, 170 FERC ¶ 61,204 (2020) ("Incentives NOPR").
[7] Incentives NOPR at P 5.

transmission investment needed to meet the future energy needs of customers and the nation.[8] WIRES also urged the Commission take final action on the Incentives NOPR in a timely and expeditious manner in order to provide a stable and adequate incentives policy for investment in major infrastructure projects and realize the economic and reliability benefits of those projects.[9]

While WIRES agrees that cybersecurity is an important part of reliability and supports the Commission's consideration of transmission incentives to counter the evolving and increasing threats to the cybersecurity of the electric grid, it is important for the Commission to ensure that its work on cybersecurity incentives not delay timely and expeditious completion of the Incentives NOPR rulemaking proceeding. As WIRES previously indicated in the Incentives NOPR, quick and decisive action by the Commission to revise its electric transmission incentives policy is needed in order to promote a sustained period of robust capital investment in transmission projects that would provide impactful and extensive economic benefits and help to address the severe economic consequences of the ongoing COVID pandemic health crisis.[10] The Commission should therefore act promptly to issue a final rule in the Transmission Incentives NOPR proceeding.

In addition, the Commission has already developed a robust and extensive record in the Incentives NOPR proceeding, including initial and reply comments on a Notice of Inquiry[11] as well as on the NOPR itself. The Commission therefore has developed a complete administrative record to support its decision-making on the Incentives NOPR. In contrast, the White Paper is

[8] Comments of WIRES, Docket No. RM20-10 (July 1, 2010) ("WIRES Initial Comments"); Reply Comments of WIRES, Docket No. RM20-10 (July 16, 2010) ("WIRES Reply Comments").
[9] Response of WIRES to Motion for Extension of Time, Docket No. RM20-10 (May 4, 2020) ("WIRES Extension Response").
[10] WIRES Extension Response at 6-7.
[11] *Inquiry Regarding the Commission's Electric Transmission Incentives Policy*, 84 FR 11759 (Mar. 28, 2019), 166 FERC ¶ 61,208 (2019) ("NOI").

only at the earliest stage of consideration for potential Commission action. Given the Commission's decision to consider cybersecurity incentives in a later, separate proceeding from the Incentives NOPR, the Commission should not allow the differing procedural postures of these bifurcated proceedings to delay final action on the Incentives NOPR.

B. WIRES Supports Appropriate ROE And Non-ROE Incentives For Cybersecurity Investments.

1. ROE Incentives

Challenges to the resilience of the nation's energy infrastructure are an ever-increasing concern. As Chairman Chatterjee observed last year in his testimony before the House Subcommittee on Energy and Commerce, the nation's "critical infrastructure is increasingly under attack" and relevant government agencies such as the Department of Homeland Security have "issued multiple public reports describing cyber-intrusion campaigns against our critical infrastructure, including the electric grid."[12] Recent estimates indicate that cyberattacks on the grid have increased 35 percent since more electric-sector employees have been working remotely from home in response to the COVID-19 pandemic.[13] And the potential consequences of a successful cyber-attack can be profound. Various studies and industry tabletop exercises have examined how cybersecurity events pose the potential for widespread, long-lasting power outages that could undermine the resilience of the nation's grid.[14] As a result, WIRES has

---

[12] Written Testimony of Neil Chatterjee before the U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Energy at 2-3 (June 12, 2019) *available at* https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Chatterjee%20%20Testimony%20of%20Neil%20Chatterjee%20for%20House%20Hearing%206.12.19.pdf.

[13] *See, e.g.*, https://www.bloomberg.com/news/articles/2020-07-30/hackers-are-targeting-the-remote-workers-who-keep-your-lights-on.

[14] ScottMadden, Inc., *Informing the Transmission Discussion: A Look at Renewables Integration and Resilience Issues for Power Transmission in Selected Regions of the United States* (Jan. 2020) at 281 (ScottMadden Report).

strongly advocated for a robust transmission grid as a central means of achieving sustained resilience and has urged the Commission to consider incentivizing utilities to be proactive in addressing cyber threats, including incentives in the form of an adder to base ROEs.[15]

Accordingly, WIRES supports the White Paper's proposal to provide ROE incentives to utilities for cybersecurity investments.[16] In particular, WIRES supports Commission Staff's proposal to authorize utilities for up to 200 basis points of ROE incentives for cybersecurity investments.[17] However, because the efficacy of an ROE incentive is determined by the amount of capitalized costs to which it is applied, and because many of the costs associated with implementing and maintaining cybersecurity investments have typically been treated as expenses rather than capitalized, ROE incentives alone may be insufficient to bolster added investment in cybersecurity protections. As discussed further below, certain non-ROE incentives, such as allowing the capitalization of costs that have historically been expensed or the creation of regulatory assets, may be needed in order for the proposed ROE incentives to have the desired impact. Moreover, while WIRES supports the proposed ROE incentives, WIRES continues to believe that it is essential for the Commission to ensure that base ROEs are set at just and reasonable levels sufficient to attract capital for investment in vital transmission infrastructure going forward;[18] it cannot rely on its incentives policies alone to achieve that objective.

2. Non-ROE Incentives

WIRES also supports the White Paper's proposal to allow applicants to seek non-ROE incentives for cybersecurity investments. The White Paper correctly notes that "[t]hese

[15] Initial Comments of WIRES at 8, Docket No. PL19-3-000 (June 26, 2019).
[16] White Paper at 13.
[17] White Paper at 22.
[18] *See*, *e.g.*, Supplemental Comments of WIRES, Docket No. PL19-4 (June 18, 2020).

incentives could reduce the financial risk associated with additional investments in cybersecurity, as they do for major transmission projects."[19] In particular, WIRES strongly supports the White Paper's proposal to allow utilities to defer and amortize certain costs that have traditionally been categorized as expenses through the creation of a regulatory asset.[20] The Commission should also explore opportunities to allow utilities to capitalize certain cybersecurity-related expenses. As noted above, this shift in cost treatment would enhance the effectiveness of the proposed ROE incentives. Many of the costs associated with cybersecurity investments are incurred on an ongoing basis to maintain the relevant systems once installed and to administer a utility's cybersecurity programs.[21] For example, training and development of the cyber workforce results in ongoing increased labor costs incurred to implement and sustain effective cybersecurity programs. Currently, the costs of maintaining and administering these programs are expensed rather than capitalized. As a result, a utility does not earn any return on these investments and any ROE incentive would not apply to these costs, which limits the effectiveness of the ROE incentive in encouraging utilities to make investments that enhance the cybersecurity of their assets. The Commission should therefore consider the underlying costs of labor, communications infrastructure to improve security, and other improvements as eligible for capitalization under its accounting standards.

Finally, because it would be administratively inefficient and burdensome for the Commission to require utilities to file individual requests with the Commission to capitalize cybersecurity investments, the Commission should allow capitalization of these costs on a self-implementing basis. In other words, the Commission should provide guidance about which

[19] White Paper at 13.

[20] White Paper at 14.

[21] *Id.*

cybersecurity-related costs it will permit utilities to capitalize such that a utility that wishes to capitalize such costs is not required to file with the Commission to obtain preauthorization.

C. Cybersecurity Incentives Should Not Be Limited In Duration Or Sunset.

The White Paper proposes that, in contrast to the Commission's treatment of incentives for other investments, incentivized cybersecurity investments should have a sunset date of no more than three to five years because of "the quickly evolving nature of cybersecurity threats and best practices."[22] WIRES opposes the White Paper's suggestion to impose a sunset on authorized cybersecurity incentives. There is simply no basis provided in the White Paper for drawing an arbitrary line in the sand at three, five, or any other random number of years as to when incentives for cybersecurity investments should terminate. It is unclear what bearing the notion that cybersecurity threats can evolve quickly has on whether a utility should be incentivized to make investments to protect against cyberthreats or whether incentives for such investments should be sunset. In any event, in many cases, cybersecurity incentives will sunset themselves due to the nature of these investments. To the extent that the benefits of cybersecurity investments correspond with the duration of the investments, any incentives should remain in place for life of the investment.

Accordingly, the Commission should not adopt any limitation on the duration of or otherwise sunset any cybersecurity incentives once granted.

D. The Proposed Reporting Requirements Should Be Modified.

The White Paper proposes requiring a utility that receives a cybersecurity incentive to make annual filings subject to audit, including "quantifiable metrics to support that the expected

[22] White Paper at 23.

enhanced cybersecurity benefits were realized."[23] WIRES opposes such a requirement. It is unclear what quantifiable metrics a utility could provide to demonstrate that a potential cybersecurity threat did not materialize because of a specific cybersecurity investment, and the White Paper offers no guidance on how a utility could develop such metrics. If the cybersecurity investments for which a utility receives an incentive are effectively implemented, they will provide the benefits that they were designed to provide. There is no need to establish additional metrics to measure the value that they provide; successful implementation is the only metric that matters. As any type of abstract, after-the-fact reporting requirement is only likely to discourage a utility from seeking a cybersecurity incentive and could ultimately frustrate the Commission's desired goal of incentivizing cybersecurity investment, it should be abandoned.

III. CONCLUSION

WIRES appreciates the opportunity to provide these comments on the Commission's White Paper and looks forward to the opportunity to further comment on any additional steps or actions the Commission decides to take.

Respectfully submitted,

/s/ *Larry Gasteiger*

_____

Larry Gasteiger
Executive Director
WIRES
1325 G Street, N.W., Suite 500
Washington, DC 20005
Office: (202) 449-7673
Cellphone: (703) 980-5750
lgasteiger@exec.wiresgroup.com

August 17, 2020

[23] White Paper at 25.