UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Incentives for Advanced Cybersecurity Investment	))	Docket No. RM22-19-000

COMMENTS TO LIMIT CHARGES TO CONSUMERS AND EXTRA PROFITS FOR TRANSMISSION UTILITIES FOR INVESTMENT IN ADVANCED CYBERSECURITY TECHNOLOGIES AND ACTIONS

BY

OFFICE OF THE OHIO CONSUMERS' COUNSEL

Bruce Weston
Ohio Consumers' Counsel

Larry Sauer
Deputy Consumers' Counsel

Office of the Ohio Consumers' Counsel
65 East State Street, Suite 700
Columbus, Ohio 43215
(614) 466-1312
larry.sauer@occ.ohio.gov

November 7, 2022

TABLE OF CONTENTS

PAGE

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Incentives for Advanced Cybersecurity Investment	))	Docket No. RM22-19-000

COMMENTS TO LIMIT CHARGES TO CONSUMERS AND EXTRA PROFITS FOR TRANSMISSION UTILITIES FOR INVESTMENT IN ADVANCED CYBERSECURITY TECHNOLOGIES AND ACTIONS BY OFFICE OF THE OHIO CONSUMERS' COUNSEL

I. INTRODUCTION AND BACKGROUND

To protect consumers from unjust and unreasonable rates, the Federal Energy Regulatory Commission ("FERC") should limit the amount, duration and availability of the transmission incentives proposed in this Notice of Proposed Rulemaking ("NOPR"). Specifically, FERC should cap such extra profits cybersecurity incentives at 50 basis points. FERC also should shorten the duration for collection from consumers from five years to a maximum of three. Moreover, the incentive should only be available for new technologies that exceed current or mandated standards. Likewise, extra payments from consumers should not be made for technologies that eventually become an industry norm.

FERC seeks by this NOPR to implement newly authorized section 219A of the Federal Power Act, 16 U.S.C. § 824s-1, passed by Congress as part of the Infrastructure and Jobs Act.[1] The new law requires FERC to make transmission incentives available to transmission utilities that make cybersecurity expenditures that enhance their security beyond what is already required. Such expenditures must improve the utility's ability to protect against, detect, respond

[1] *Incentives for Advanced Cybersecurity Investment,* Notice of Proposed Rulemaking, 180 FERC ¶ 61,189 at P 1 (2022) ("NOPR"), citing Publ. L. 117-58, section 40123.

to, or recover from a cybersecurity threat to the benefit of consumers and national security. NOPR at P 1. The incentives are also to be made available to utilities that participate in cybersecurity threat information sharing programs. *Id.*

The Office of the Ohio Consumers' Counsel ("OCC") represents the interests of Ohio residential consumers who receive electric service from investor-owned utilities that participate in PJM Interconnection's electric grid management services. OCC supports FERC's efforts to protect electric consumers by protecting critical energy infrastructure from cybersecurity threats. FERC is obligated by the new law to provide incentives for certain investments and actions related to cybersecurity. However, in implementing the statute, FERC must keep in mind that transmission utilities are already required by several mandatory Critical Infrastructure Protection ("CIP") reliability standards to undertake actions to protect their systems from cybersecurity threats.[2] And these utilities are able to recover the costs related to these mandatory standards. In addition, business standards already adopted by the North American Energy Standards Board ("NAESB") similarly address cybersecurity mandates, and are incorporated into transmission utility tariffs as required in Order No. 676-J.[3]

To the extent the current CIP standards are insufficient to provide adequate reliability protection for the nation's electric transmission grid, FERC should direct the North American Electric Reliability Corporation ("NERC"), NAESB and the industry to work collaboratively to

---

[2] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, at P 1, *order on reh'g and clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*¸ Order No. 706-B, 126 FERC ¶ 61,229, *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[3] *See, e.g.*, *Standards for Business Practices and Communication Protocols for Public Utilities,* Order No. 676-J, 175 FERC ¶ 61,139 at P 2 (2021) ("The WEQ Version 003.3 Standards include revisions related to the surety assessment on cybersecurity performed by Sandia National Laboratories (Sandia) designed to strengthen the practices and cybersecurity protections established within the standards.") At P 11, FERC states that "NAESB reports that the changes strengthen the practices and cybersecurity protections established within the standards by aligning security requirements with other cybersecurity guidelines, mitigating potential vulnerabilities, and incorporating more secure communication and encryption methodologies."

update and implement new mandatory standards and business practices. FERC must be careful to not let incentives become the only means of staying up to date with needed state-of-the art protections against cybersecurity threats. Such a regulatory construct could result in extra, unnecessary charges to consumers by encouraging gold-plating spending for imprudent facilities and through over payments for extra unneeded profits. Consumers should not have to pay charges for imprudent or unnecessary facilities and extra profits to utilities to keep their grid protections systems up-to-date to counter fast-evolving cybersecurity threats.

Cybersecurity threats are not unique to the electric utility industry. Every aspect of the United States' economy faces an increasing number of rapidly changing cybersecurity threats. Investing in technologies and actions to protect against such threats should be a due-diligence responsibility and best practice of every major industry in the nation, including the utility industry. Cybersecurity threats may be constantly evolving to evade existing technologies and programs. But that means that existing technology mandates to protect against such threats should similarly evolve where once-advanced protections become the norm. The NOPR's proposal to award a 200-basis point adder to a utility's Return on Equity ("ROE") would be an unwarranted and excessive level of extra profits to transmission utilities for doing what is already in the industry's best interest – to keep billions of dollars of their investment in electric infrastructure safe from new and evolving cybersecurity threats.

OCC commends FERC for its inquiry into the incentives needed to encourage transmission utilities to meet and protect against evolving cybersecurity threats. However, FERC should limit the amount of the incentives, the duration that the incentives are available, and the scope of activities that would warrant the incentives to safeguard that the extra profits paid is no greater than that needed to encourage the desired behavior. The incentives should be limited to

ROE adders of no greater than 50 basis points. FERC should limit the duration of the incentives to the lesser of (a) three years, (b) the life of the assets for which the incentive is provided, or (c) the date on which such technologies or actions become obsolete or routine in the industry or become a new mandated standard. FERC also should limit the incentive to those transmission utilities that have complied with existing mandatory reliability standards. A utility should not be allowed to earn excess profits for investment in new activities if has not complied with existing mandatory standards.

Moreover, FERC should not grant incentives in any situation in which a utility is already required by current mandatory CIP reliability standards, NAESB business standards, federal, state or local laws, regulations or orders to undertake those investments or activities. Utilities should not be compensated for mandates that are already required. FERC also should not allow deferred regulatory asset treatment for any expenses on cybersecurity protection. And FERC should reject the concept of performance-based rates for this incentive. Neither approach has been shown to be practical or reasonable given the potential magnitude of the involved expenses.

II. COMMENTS

A. To protect consumers, FERC should adopt strict eligibility rules for qualifying for the advanced cybersecurity incentives.

1. While FERC should adopt the two proposed eligibility criteria, it should add a third criteria that would require an applicant for an advanced cybersecurity incentive to be compliant with existing Critical Infrastructure Protection mandatory reliability standards.

OCC supports the NOPR proposal (NOPR at P 20) to adopt two primary eligibility criteria for receipt of the advanced cybersecurity incentives. First, the advanced technology or action must *materially* improve the cybersecurity of the utility's transmission facilities. Second, the incentives should be limited to advanced cybersecurity technologies and participation in cybersecurity threat information sharing programs that are not already required by federal, state

or local laws, orders, regulations or mandatory business practices standards. FERC should only authorize incentives for truly voluntary investments or actions taken to install more advanced cybersecurity technology that benefits consumers. FERC also should require the utilities to demonstrate that the advanced technologies and/or participation in cybersecurity threat information sharing programs provide quantifiable, incremental benefits for consumers that will exceed their costs.

In *The Dayton Power & Light Co.*,[4] FERC made clear that utilities should not be paid incentives for taking actions that are already required by law.[5] Quoting the Ninth Circuit Court of Appeals in *Cal. Pub. Util. Comm'n v. FERC*,[6] FERC stated that the Ninth Circuit found that the "incentive cannot induce behavior that is already legally mandated," and thus "the voluntariness of a utility's membership in a transmission organization is logically relevant to whether it is eligible for an [RTO Participation] adder."[7] FERC concluded that "[c]onsistent with that longstanding policy, we do not believe it would be appropriate to award an incentive for an action that the requesting entity is required by law to take even where that action comes with substantial benefits or risks."[8]

This ruling is consistent with the District of Columbia Circuit Court of Appeals mandate in *City of Detroit*[9] that FERC must make sure that "the increase is in fact needed, and no more than is needed for that purpose." Applying this principle in C*ity of Charlottesville v. FERC*,[10] the

[4] *The Dayton Power and Light Co*., 176 FERC ¶ 61,025 (2021) ("*Dayton*").

[5] *Id.* at P 27.

[6] *Cal. Pub. Util. Comm'n v. FERC*, 879 F.3d 966 (9th Circuit 2018) ("*CPUC"*).

[7] *Dayton* at P 27, citing *CPUC* at 975, citing Order No. 679-A, 117 FERC ¶ 61,345 at P 86.

[8] *Dayton* at P 30.

[9] *City of Detroit*, 230 F.2d at 817.

[10] *City of Charlottesville,* 661 F.2d at 954.

D.C. Circuit Court found insufficient evidence to support FERC's finding that the tax savings in that case that were not directly reinvested in the utility would eventually "trickle down" from the corporate parent to its exploration and development affiliates, resulting in increased gas supply benefits for consumers. The Court determined that FERC cannot just ask this Court "to take it on faith that such funneling of tax savings does occur."[11] In other words, FERC must make sure there is a link between the incentive to be provided and the consumer benefits to be gained from that incentive.

Given these precedents, OCC supports FERC's proposal (NOPR at P 29) that there should be no incentives for investments in advanced technologies required by the NERC Critical Infrastructure Protection Reliability Standards. For the same reason, FERC also should not allow incentives for investment in any advanced cybersecurity technology that is required by federal, state or local orders, *e.g.,* orders in merger proceedings that impose a requirement to engage in such technologies or actions as a condition of authorization for the merger. NOPR at PP 20, 22.

There also should be no incentive for utilities already participating in cybersecurity threat information sharing programs. NOPR at P 41. None of these situations would comport with the mandates of *Dayton*, *CPUC*, *City of Detroit* and *City of Charlottesville*. FERC must safeguard there is some incremental benefit to consumers to justify any incentive. There is no incremental benefit associated with actions taken prior to the availability of the incentive. In that situation, the utility is simply complying with mandates already required by federal, state or local laws or court and regulatory orders.

FERC should add a third eligibility criteria to the final rule. It should require that any utility seeking an advanced cybersecurity incentive must be in compliance with all existing

[11] *Id.*

mandatory Critical Infrastructure Protection Reliability Standards and North American Energy Standards Board tariff requirements. It would make no sense to reward a transmission utility for a voluntary investment in advanced cybersecurity technology if the utility is not compliant with existing cybersecurity mandates. FERC 2022 Staff Report on Lessons Learned from Commission-led CIP Reliability Audits,[12] in the Lessons Learned discussion, found that:

a. although most entities established policies, procedures and controls consistent with CIP-003-8, Requirement R2, some programs could benefit from regular re-evaluations to ensure continued effectiveness;[13]
b. some entities did not have sufficient end-of-life or end-of-service management programs for cyber assets, creating potential security and compliance risks;[14]
c. some utilities inconsistently implemented processes and controls to deter, detect and prevent malicious code within the CIP environment;[15]
d. some utilities did not include key elements in the execution of the vulnerability assessment processes intended to detect unencrypted communications and avoid interception, reply, adversary-in-the-middle and injection attached which could otherwise be mitigated;[16]and
e. some utilities undertook insufficient investigations of third-party providers of software for vulnerabilities and malicious code on devices used to transmit data.[17]

FERC should not be awarding excess profits to utilities that do not comply with the current mandatory Critical Infrastructure Protection Reliability Standards. FERC should require transmission utilities to demonstrate in applications for incentives for advanced cybersecurity technologies that they are already in compliance with existing mandatory standards. Otherwise, FERC would be encouraging utilities to shun investments in mandatory activities for the greater

[12] 2022 Staff Report on Lessons Learned from Commission-Led CIP Reliability Audits, prepared by Staff of the Federal Energy Regulatory Commission Washington D.C. (Oct. 14, 2022) (Staff CIP Audit Report"), available at https://www.ferc.gov/media/2022-staff-report-lessons-learned-commission-led-cip-reliability-audits.

[13] Staff CIP Audit Report at 10-11 (citing as one example the failure of some utilities to implement controls to mitigate the risk of malicious code transfer to Bulk Electricity System ("BES") cyber electronic devices used for data transfer, vulnerability assessment, maintenance or troubleshooting purposes).

[14] *Id.* at 13.

[15] *Id.* at 15.

[16] *Id.* at 17.

[17] *Id.* at 19.

rewards to be had by investment in "voluntary" cybersecurity activities. The utility must be required to demonstrate that it satisfies the current threshold for mandatory protection from cybersecurity threats before being rewarded for voluntary investments and activities.

2. To protect consumers, FERC should adopt a pre-qualification list of cybersecurity technologies and actions that qualify for incentives but should update that list periodically.

FERC's proposed approach of adopting a list of technology investment that would presumptively qualify for an incentive makes sense. The creation of a list would provide greater transparency regarding the eligibility of various technologies and actions for incentives. It potentially provides a benefit in reducing litigation over incentive requests. However, FERC must provide an opportunity for interested stakeholders to comment on any technologies or actions proposed for additions or deletions to such a list through a rulemaking proceeding. The proposed presumption of eligibility associated with the pre-qualification list means that FERC must first make certain that the advanced technologies added to or deleted from the list are appropriate. That is, they must consist of truly advanced technologies that are not obsolete or routine in the industry and that provide a cost-benefit savings for consumers.

FERC also should periodically update the pre-qualification list to remove technologies that have become standard over time and/or that have been adopted as additional mandatory CIP reliability standards or NAESB business practices. Eligibility for incentives should be limited to those advanced technologies and actions that will go above and beyond current mandatory or accepted practices in the industry to protect consumers. Utilities should not receive additional profits for merely taking steps that are routine or are already considered best practices in the industry. The goal should be to incentivize adding additional security to protect consumers. Any final rule should make clear that FERC will remove any technology or action from the presumptive list of items eligible for incentives if they become an industry norm. FERC should

then require every utility receiving incentives for those technologies or actions to show cause why the incentive should not be terminated as of the date of the show cause order. NOPR at P 31.

In addition to the pre-qualification list approach, FERC should implement a case-by-case approach to review any requests for incentives for new technologies that are not included on the pre-qualification list. NOPR at PP 19, 32. FERC's ratemaking policy for routine expenses recognizes that:

> the company's obligation to include the costs in its cost-of-service for ratemaking purposes *as soon after their incurrence as possible*, in order that a decision could be made whether the current body of ratepayers should be charged for their recovery. A regulated company is not permitted to "sit" on costs, delaying their inclusion in the claimed cost of service until it believes the time is auspicious to seek their recovery.[18]

The reasoning behind this policy acknowledges that customers should have an opportunity for timely review of the prudency of expenses; make sure that customers on the system today pay for expenses incurred on their behalf; and prevent the potential for double recovery of these costs in the future.[19] There should be no presumptions of eligibility for any technology or action that is not included on the pre-qualification list through a rulemaking process. NOPR at P 32.

FERC also should require that any incentive application (whether an application for incentives for advanced technologies and actions on the pre-qualification list or for incentives that are not included on that list) should be made in a FPA section 205 filing. FERC should further require that both types of applications explicitly identify in which accounts the utility will

[18] *Va. Elec. & Power Co.*, 15 FERC ¶ 61,052 at 61,113, *on reh'g*, 17 FERC ¶ 61,150 (1981); *see also FirstEnergy Services Co.,* 110 FERC ¶ 61,230 (2005) ("*FirstEnergy*").

[19] *Id.*

book the costs associated with the investment, expense or action. Such a requirement is needed to ensure transparency and proper rate treatment for these investments.

B. FERC's proposed 200 basis point ROE adder and regulatory asset deferral treatment for certain expenses are unjust and unreasonable for developing rates to charge consumers.

1. To protect consumers, FERC should not allow cybersecurity expenses to be treated as a regulatory asset.

OCC opposes FERC's proposal to allow deferred accounting and recovery of a return on the unamortized portion of the costs for cybersecurity expenses. NOPR at P 39. FERC states that certain cost categories, such as software, that were historically purchased by utilities may now be procured through periodic payments to vendors that are recorded as expenses. *Id.* Additional costs that FERC is proposing be eligible for deferred cost recovery treatment include expenses associated with employee training to implement new cybersecurity practices, internal system evaluations and assessments by third parties, and on-going dues for participation in cybersecurity threat information sharing programs. NOPR at P 40. However, that proposal would only allow utilities to capitalize expenses, forcing customers to pay a return, or profit, to the utility for the expense. Deferred accounting and cost collection of cybersecurity expenses as regulatory assets will cost consumers more over time than would recovery of the expense all in one year. Some of these expenses may be relatively small and thus would be unlikely to add much to the rates consumers must pay even if expensed in one year. It does not make sense to charge consumers even more over time by allowing collection of a return on these expenses from consumers.

FERC has allowed regulatory asset treatment of a one-time expense of considerable magnitude to avoid rate shock, *e.g.,* the significant vegetation management expenses incurred in the wake of the 2003 black out required by FERC's 2004 Policy Statement on Matters Related to

Bulk Power System Reliability.[20] However, that authority was not automatic. FERC still required the utilities to file for authorization for the regulatory asset treatment in order to make sure utilities were not double recovering their annual routine vegetation management expenses.[21] Moreover, the decision to allow regulatory asset treatment for vegetation management expenses was premised on a determination that the expense was a one-time event. In contrast, many cybersecurity expenses are likely to be routine, on-going expenses, *e.g.,* payments to third parties for monitoring of cybersecurity threats or participation in cybersecurity information sharing programs. These routine, on-going expenses are not suitable for treatment as regulatory assets

FERC should reject the proposal to provide a regulatory asset incentive for collection of cybersecurity expenses from consumers. However, if FERC decides otherwise, it should set a threshold above which any annual expense must exceed to qualify for regulatory asset treatment. Such threshold, for example, could be set at an expense level that exceeds $10 million in one year.

Additionally, the same expense should not qualify for both the ROE adder and regulatory asset treatment. FERC states that it preliminarily finds that "the same expenditure should not be eligible for both the Cybersecurity ROE Incentive and the Regulatory Asset Incentive." NOPR at P 38. However, FERC then states that if costs are allowed to be deferred as a regulatory asset, they "should be included in rate base for a determination of the base return, but not for the additional return associated with the 200-basis point ROE adder." *Id.* This statement appears to contemplate a situation in which the same expense could be eligible for both the Cybersecurity

[20] *FirstEnergy,* 110 FERC ¶ 61,230 at PP 16-17; *Policy Statement on Matters Related to Bulk Power System Reliability*, 107 FERC ¶ 61,052, PP 27-28 (2004) ("2004 Reliability Policy Statement"), *supplemented*, 110 FERC ¶ 61,096 (2005).

[21] *FirstEnergy*, 110 FERC ¶ 61,230 at PP 16-17.

ROE Incentive and the Regulatory Asset Incentive because it contemplates that the expense could receive both incentives. It appears that FERC is contemplating that in calculating the Regulatory Asset Incentive, the 200-basis point ROE adder would not be included in the regulatory asset balance. However, Congress never intended that one expense could receive both the Cybersecurity ROE Incentive and the Regulatory Asset Incentive. FPA Section 219A(e)(2) requires that "Any rule issued pursuant to this section shall preclude rate treatments that allow unjust and unreasonable *double recovery* for advanced cybersecurity technology."[22] FERC should clarify the ambiguity in the NOPR by clarifying that a utility can receive *either* the Cybersecurity ROE Incentive or the Regulatory Asset Incentive – but not both.

2. A 200-basis point Return on Equity adder is unjust and unreasonable for charging consumers.

FERC's proposal to provide a 200-basis point ROE adder for investment in advanced cybersecurity technologies or activities is not just and reasonable. A 200 basis-point ROE adder is significantly higher than the 100-basis point and 150 basis point ROE incentive adders contemplated in Order No. 679,[23] FERC's existing transmission incentives policy. Most perceived risks associated with cybersecurity threats have long since been incorporated into utility ROEs.[24] Shareholders already are being compensated through the base return on equity for most of the risk for such investments. FERC provided no evidence, or even a reasonable explanation justifying a 200-basis point ROE adder proposal.

---

[22] 16 U.S.C. s 824s-1(e)(2) (emphasis added).

[23] *Promoting Transmission Investment Through Pricing Reform*, Order No. 679, FERC Stats & Regs. ¶ 31,222; *order on reh'g*, Order No. 679-A, 117 FERC ¶ 61,345 (2006).

[24] *See, e.g., Promoting Transmission Investment Through Pricing Reform*, Policy Statement, 141 FERC ¶ 61,129 at P 11 (2012) ("Transmission Incentives Policy Statement") ("The Commission authorizes a company's base ROE utilizing a range of reasonableness resulting from a discounted cash flow (DCF) analysis that is applied to a selected proxy group representing firms of comparable risk. The resulting base ROE authorized by the Commission is designed to account for many of the risks associated with transmission investment and to support that investment").

The cost of an investment in any particular advanced cybersecurity technology or activity is likely to range depending on the complexity of the technology or activity. Instead of proposing a flat 200-basis point ROE adder, FERC should provide for a pool of potential adders, ranging from 25 basis points up to a cap of 50 basis points depending on the magnitude of the investment and the complexity or proven track record for the technology or activity. In essence, FERC should require that utility to demonstrate increasingly greater benefits to consumers from the proposed advanced technologies or activities to be eligible for the higher level of incentives. A 200-basis point adder is not necessary and is unreasonably costly for consumers. It also defies the logic of Order 679, which provided higher ROEs for more complicated and expensive transmission projects.[25]

3. To protect consumers, FERC should set the upper end of the range of reasonableness as a cap on total ROE incentive adders plus base ROE for a utility.

One critical element of Order No. 679 is missing from the cybersecurity NOPR. In the transmission incentives provided under Order No. 679 and FPA section 219, FERC imposed a cap on the combination of the Order No. 679 ROE adders and the base ROE set at the upper end of the zone of reasonableness authorized for the utility.[26] That cap should remain in place for the cybersecurity incentive The utility's base ROE and all of its ROE adder incentives, including the advanced cybersecurity incentive, should not exceed the upper end of the range of reasonableness authorized for the utility. New FPA section 219A, like FPA section 219 before it, requires that "[a]ny rate approved under a rule issued pursuant to this section, including any revisions to that rule, shall be subject to the requirements of sections 824d and 824e of this title

[25] Transmission Incentives Policy Statement at P 17.

[26] Order No. 679 at P 93.

that all rates, charges, terms, and conditions—(A)shall be just and reasonable; and (B)shall not be unduly discriminatory or preferential."[27] FERC should protect consumers by setting the overall upper end of the zone of reasonableness as a cap in any final rule for advanced cybersecurity incentives.

4. To protect consumers, FERC should not allow performance-based rates for advanced cybersecurity investments and activities.

FERC seeks comment on whether to allow a performance-based rate approach to investment in advanced cybersecurity technology and activities. NOPR at P 44. OCC urges FERC to not allow a performance-based rate approach as an incentive for advanced cybersecurity investments and expenses. Such an approach would require the establishment of a threshold beyond which the utility is expected to perform to safeguard against providing incentives for routine or best practices type activities undertaken by most utilities. Setting that performance threshold for advanced cybersecurity investment and activities is likely to be challenging given the rapid pace of development in both the types of cybersecurity threats experienced and the technological advances used to counter those threats. This rapid pace of evolution does not allow sufficient experience to be gained with new, advanced technologies to be able to appropriately gauge whether the utility is performing at a higher level than some average threshold of utilities.

[27] 16 U.S.C. s 824s-1(e)(1).

C. To protect consumers from unwarranted charges incentives should be limited to the earlier of three years; the end of the depreciable life of the asset; the date on which the investment is mandated by federal, state or local laws, orders or regulations; or the date on which the technology or action is removed from the pre-qualification list.

FERC proposes to allow a utility to receive a cybersecurity incentive until the earliest of (1) the conclusion of depreciation life of the underlying asset; (2) five years from when the investment enters service; (3) the time that the technology or activity becomes mandatory pursuant to a Reliability Standard approved by FERC, or by federal state or local law; or (4) the recipient no longer meets the requirements for receiving the incentive. NOPR at P 46. FERC should limit the five-year duration proposal to a maximum of three-years. The rapid pace of evolving cybersecurity threats and technological advances in efforts to combat those threats justifies a three-year limit on receipt of the cybersecurity incentive. Consumers should not be required to continue paying extra profits for investments and activities that may become obsolete or routine in the industry. This also applies to the deployment of cybersecurity facilities that are or become mandated by federal, state, or local law or regulatory action. The intent of the incentive is to encourage activity by the utility. Continuing to provide that incentive once the technology or investment becomes obsolete or routine would no longer satisfy the *City of Detroit* mandate that the incentive be no larger than is needed to induce the required behavior.[28]

Transmission utilities should be incented to invest in new, emerging technologies to protect consumers from cyber threats. Providing a permanent extra profit payments from consumers for technologies or actions taken in the past will not encourage additional investment in new technologies or actions in the future. Investment in those new technologies and actions will be encouraged by the inclusion of such technologies and actions on the Pre-Qualification

[28] *City of Detroit,* 230 F.2d at 817.

List. Continuing to give incentives for past actions that have become obsolete or routine or that have been removed from the pre-qualification list would only provide windfall profits for action already taken, contrary to the mandates of the Ninth Circuit in *CPUC*. Moreover, FERC should not allow a utility to receive overlapping incentives for investment in new technology intended to achieve the same benefits intended under an existing incentive. There must be quantifiable, *incremental* benefits that can be measured in cost-benefit savings to consumers.

D. For transparency and consumer protection, FERC should impose periodic reporting requirements.

FERC proposes to require a utility receiving a cybersecurity incentive under the NOPR to submit informational reports for the duration of the incentive. NOPR at P 54. OCC strongly supports this proposal. Consumers will be paying the utility a higher level of profits for years for investment in advanced cybersecurity technology and activities intended to benefit them by protecting the transmission grid from damaging cybersecurity threats. FERC and consumers must both be able to verify that the investments are being made and that the intended benefits are being received. The only way FERC can continue to make certain that the incentive remains just and reasonable is require the utility to demonstrate an overall cost-benefit to consumers to justify the expense. As FERC notes in the NOPR, it must safeguard against requiring consumer to pay extra profits for on-going services, routine system maintenance, surveillance and other routine labor costs. NOPR at P 55. These reports will be especially important if FERC approves a duration for the incentive of longer than three years.

III. CONCLUSION

FERC should protect consumers from bearing the cost of unnecessary incentives, and thus paying a transmission utility extra profits for investment in routine or already-mandated advanced cybersecurity technologies or for already-mandated cybersecurity threat information

sharing programs. FERC should (a) limit the Cybersecurity ROE Incentive to no more than 50 basis points; (b) allow for a range of incentives between 25 and 50-basis points depending on the complexity of the technology or magnitude of the expense. FERC also should limit the availability of the incentive to the earlier of three-years; the end of the asset's depreciation life; the date that the technology or activity becomes mandatory pursuant to FERC-approved Reliability Standards or federal, state or local laws; or the date the technology or activity is removed from the pre-qualification list. Eligibility for the Cybersecurity ROE Incentive should be limited to investments or actions that are not already required by mandatory CIPS Reliability Standards or NAESB business practices. FERC should not allow advanced cybersecurity technology incentives to any utility that is not in full compliance with existing mandatory CIP Reliability Standards. FERC should not allow use of a regulatory asset deferral for cybersecurity expenses. And FERC should reject the concept of performance-based rates for cybersecurity expenses; and should annually review and update the list of presumptively approved technologies and actions eligible for the ROE Incentive. Finally, FERC should require mandatory annual reporting by utilities receiving the asset for the duration of the time the utility is receiving the incentive.

Respectfully submitted,

Bruce Weston
Ohio Consumers' Counsel

/s/ Larry Sauer
Larry Sauer
Deputy Consumers' Counsel

Office of the Ohio Consumers' Counsel
65 East State Street, Suite 700
Columbus, Ohio 43215
(614) 387-2965
Larry.sauer@occ.ohio.gov

February 7, 2022

CERTIFICATE OF SERVICE

I hereby certify that I have on this date served a copy of the foregoing document via electronic mail upon all parties of record on the Commission's official service list in this proceeding.

Dated in Columbus, Ohio this 7th day of November 2022.

/s/ Larry Sauer
Larry Sauer
Deputy Consumers' Counsel

Office of the Ohio Consumers' Counsel
65 East State Street, Suite 700
Columbus, Ohio 43215
(614) 387-2965
Larry.sauer@occ.ohio.gov