UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives Docket No. RM21-3

**Comments of Public Citizen, Inc.**

Established in 1971, Public Citizen is a national, not-for-profit, non-partisan, research and advocacy organization representing the interests of household consumers. We are active before FERC promoting just and reasonable rates, and supporting efforts for utilities to be accountable to the public interest. Our financial details are located at our web site.[[1]](#footnote-1)

As an organization dedicated to advocacy on behalf of households, Public Citizen fully appreciates that consumers can benefit from investments in cybersecurity protections, and we encourage utilities to make outlays that go above and beyond federal minimum requirements. But as cybersecurity challenges and corresponding investment needs quickly mount, it is unjust and unreasonable to expect consumers to bear all of the responsibility of looming cybersecurity defense needs. **Shared financial responsibility among shareholders and owners of utility infrastructure, federal and sub-federal governments, and consumers is necessary to ensure equitable investments for needed cybersecurity enhancements.**

Importantly, benefits from increasing spending on cybersecurity protections will be diluted if utilities have poor compliance track records. We must *spend smarter*, with only those utilities with stellar compliance histories allowed to recover voluntary cybersecurity investments from ratepayers. Providing lucrative cost recovery for cybersecurity investments by utilities with poor compliance practices will result in increased consumer costs with no improved security benefits. Indeed, as Dr. Ron Ross, a Fellow with the National Institute of Standards and Technology recently noted:

As a nation, **we are spending more on cybersecurity today than at any time in our history**, while simultaneously continuing to witness an **increasing number of successful cyberattacks and breaches by nation states, terrorists, and hacktivists** that are stealing our intellectual property, national secrets, and private information. The situation is not getting demonstrably better over time and will have a debilitating long-term effect on both the economic and national security interests of the United States.” [emphasis added][[2]](#footnote-2)

For consumers, it is preferable for the Commission to work with the North American Electric Reliability Corporation (NERC) to increase minimum standards rather than rely on incentives to prompt utilities to invest in needed cybersecurity upgrades.

Cybersecurity enhancements and investment incentives for utilities are currently a top priority of the Biden Administration, the U.S. Department of Energy, and other federal agencies. Any voluntary investment proposal promoted by FERC should be closely coordinated with the U.S. Department of Energy and its existing and forthcoming grant programs, as well as with state regulatory initiatives. Consumers should not be financially liable for cybersecurity investments if existing programs outside of FERC are providing investment opportunities or regulatory mandates.

Finally, we urge governance improvements at NERC to ensure balanced stakeholder representation for cybersecurity standards development, implementation and enforcement.

**Introduction**

The Commission is proposing incentive-based rate treatments to encourage voluntary cybersecurity investments by public utilities that exceed mandated minimum standards, including a Return on Equity (ROE) adder of 200 basis points, as well as opportunities for deferred cost recovery. Each approach would provide very lucrative financial incentives for utilities to proactively make additional investments in cybersecurity systems. ROE adders and deferred cost recovery are cost-of-service incentives ultimately paid for by end consumers.

**Public Citizen Comments**

Cybersecurity threats to utility systems are rising exponentially. An August 2019 GAO report detailed the increase in these risks, and recommended FERC to increase cybersecurity standards and ensure greater compliance with those standards, without mention of reliance on financial incentives to encourage voluntary investments.[[3]](#footnote-3) This GAO report was followed by another in March 2021 detailing cybersecurity risks to state-jurisdictional electric utility distribution networks.[[4]](#footnote-4)

Existing Commission policies—through formula rates and the presumption of prudence—provide enough margin for utilities to recover expenses. As then-Commissioner Rich Glick (now Chairman) noted at the March 28, 2019 technical conference on cybersecurity investments: [existing] “cost recovery at the state or federal level really isn't a barrier to utilities doing what they need to do to protect, you know, at least from physical or cyberattacks, I think that's pretty clear.”[[5]](#footnote-5)

ROE adders and deferred cost recovery are not needed for utilities to enhance cybersecurity defenses, as utilities have already informed the Commission that existing rate recovery options are adequate. Utilities are by and large already making cybersecurity enhancements because they are attractive, low risk investments.

The utility Dominion recently informed FERC that “[w]ith respect to cost recovery for security infrastructure investments . . . the discussion during the technical conference revealed few current impediments to cost recovery in either the electric or gas industries.”[[6]](#footnote-6) Other utilities agreed that current rate recovery mechanisms are adequate: “Exelon believes that the Commission’s existing policies and mechanisms reasonably allow owners and operators of energy infrastructure to recover the costs of their physical and cyber security investments. Exelon has and plans to continue to invest in the physical and cyber security of its assets and will further improve its infrastructure to mitigate any additional threats that the Commission or DOE identifies.”[[7]](#footnote-7).

The NOPR comes at a time when the federal government is moving aggressively to mitigate perceived cybersecurity threats to critical infrastructure. The media reports that top Biden Administration officials, including Energy Secretary Jennifer Granholm and Deputy National Security Adviser Anne Neuberger, briefed top utility industry executives on March 16, 2021 on the Administration’s plan to safeguard the U.S. utility sector from cybersecurity threats and attacks.[[8]](#footnote-8)The Department of Energy has stated its commitment to ramp up cybersecurity protections in the energy system, committing new programs to achieve its objectives[[9]](#footnote-9). In a blueprint released last month, DOE’s cybersecurity office revealed that the U.S. “energy infrastructure and digital supply chain present a key target for cyber compromise” and that the “frequency and sophistication” of cyberthreats are increasing. [[10]](#footnote-10)

The federal government should play in incentivizing voluntary cybersecurity enhancements. Indeed, the U.S. Department of Energy’s *Multiyear Plan for Energy Sector Cybersecurity* notes that:

*About 90% of the nation’s energy infrastructure is owned and operated by the private sector. Today’s cyber threats may now exceed industry’s expertise, resources, and capabilities.* ***The security and integrity of the energy infrastructure is also a federal government concern because energy underpins the operations of every other critical infrastructure, the economy, and public health and safety. Because of this, ensuring the cybersecurity of energy systems is a shared responsibility between the private sector and all levels of government****.* [emphasis added][[11]](#footnote-11)

Moreover, increasing standards does not necessarily translate into higher security if there is poor cybersecurity compliance by utilities. Any approval of incentive rate treatment should be conditional on the utility’s track record of cyber security compliance, thus ensuring that there is an actual connection between making an investment and being compliant.

The NOPR problematically divulges that the Commission *may* conduct periodic verification to assess cybersecurity investments and expenses for which it has approved incentives.[[12]](#footnote-12) We believe that is not enough, as the Commission must establish a system of mandatory verification, including directing further informational filings and conducting audits.

NERC has been designated by the Commission as the Nation’s Electric Reliability Organization, and as such establishes and enforces cybersecurity standards. NERC’s current governance structure limits public interest participation in NERC’s activity. Last month, Public Citizen submitted comments to the Commission on how to improve NERC’s operations, activities, oversight and procedures, including requiring a bona fide consumer advocate to serve on the Board of Trustees.[[13]](#footnote-13) Given the NOPR’s suggestion of having ratepayers cover voluntary cybersecurity investments, the Commission’s new Office of Public Participation[[14]](#footnote-14) should include responsibilities to coordinate outreach to the public and consumer advocates on these and other NERC cybersecurity related proceedings, public comment opportunities, and stakeholder committee participation.

**Conclusion**

Utilities can rely on existing cost-of-service rate treatment to fund voluntary cybersecurity investments and do not require incentives such as ROE adders or deferred cost recovery. Preventing cybersecurity attacks is a shared financial responsibility among utilities, consumers and the government, and therefore consumers should not be responsible for shouldering all of the investment burden. FERC should improve minimum cybersecurity standards rather than rely on incentive rate treatment for voluntary investments. The development and enforcement of cybersecurity standards by NERC will be enhanced by implementing governance reforms at NERC, including placing a bona fide consumer advocate on the Board of Trustees.

Respectfully submitted,

Tyson Slocum, Energy Program Director

Pau Ruiz Guix, Research Intern

Public Citizen, Inc.

215 Pennsylvania Ave SE

Washington, DC 20003

(202) 588-1000

tslocum@citizen.org

pguix@citizen.org

1. [www.citizen.org/about/annual-report/](http://www.citizen.org/about/annual-report/) [↑](#footnote-ref-1)
2. U.S. Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*, March 2018, page 19, www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20\_0.pdf [↑](#footnote-ref-2)
3. *Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332, www.gao.gov/assets/gao-19-332.pdf [↑](#footnote-ref-3)
4. *DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81, https://www.gao.gov/assets/gao-21-81.pdf [↑](#footnote-ref-4)
5. Technical Conference Transcript at 187:22-25, Security Investments for Energy Infrastructure, Docket No. AD19-12 (Apr. 26, 2019). [↑](#footnote-ref-5)
6. Post-Technical Conference Comments of Dominion Energy Services, Inc. at page 2, Docket No. AD19-12 (May 28, 2019). [↑](#footnote-ref-6)
7. Post-Technical Conference Comments of Exelon Corporation at page 1, Docket No. AD19-12 (May 28, 2019). [↑](#footnote-ref-7)
8. Jennifer Jacobs & Jennifer A Dlouhy, “Biden Team Boosts Effort to Shield U.S. Power Grid From Hackers,” March 28, 2021, *Bloomberg*, www.bloomberg.com/news/articles/2021-03-28/biden-team-boosts-effort-to-shield-power-grid-from-cyber-threats [↑](#footnote-ref-8)
9. [www.energy.gov/articles/doe-announces-cybersecurity-programs-enhancing-safety-and-resilience-us-energy-sector](https://d.docs.live.net/Users/pauruizguix/Library/Containers/com.microsoft.Word/Data/Downloads/www.energy.gov/articles/doe-announces-cybersecurity-programs-enhancing-safety-and-resilience-us-energy-sector) [↑](#footnote-ref-9)
10. [www.energy.gov/sites/prod/files/2021/01/f82/20200112\_CESER%20Blueprint%202021\_FINAL\_508.pdf](https://d.docs.live.net/Users/pauruizguix/Library/Containers/com.microsoft.Word/Data/Downloads/www.energy.gov/sites/prod/files/2021/01/f82/20200112_CESER%20Blueprint%202021_FINAL_508.pdf) [↑](#footnote-ref-10)
11. March 2018, at page 12, www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20\_0.pdf [↑](#footnote-ref-11)
12. At 66. [↑](#footnote-ref-12)
13. *Comments by Public Citizen to improve public interest participation for America’s Electricity Grid Reliability Coordinator*, Docket No. RM21-12, March 1, 2021, www.citizen.org/article/comments-to-improve-public-interest-participation-for-americas-electric-grid-reliability-coordinator/ [↑](#footnote-ref-13)
14. FERC Docket No. AD21-9. [↑](#footnote-ref-14)