UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives	**)**	**Docket RM21-3-000**

Comments submitted to FERC on April 6, 2021
by the Foundation for Resilient Societies

The Foundation for Resilient Societies ("Resilient Societies") supports the proposed rulemaking to establish rules for incentive-based rate treatments for voluntary cybersecurity investments by public utilities and other utilities whose rates are under FERC jurisdiction. The current system of mandatory Critical Infrastructure Protection (CIP) standards implements Section 215 of the Federal Power Act. However, fast-evolving cyber-threats to the Bulk Power System (BPS) are outpacing the deliberate and incremental standard-setting process envisioned by Congress when the Act was amended in 2005. Resilient Societies applauds FERC and its staff for taking a more proactive approach to countering the dynamic cybersecurity threat environment. There are two key points we wish to make in this filing:

1. Today's threat environment can be better addressed by a combination of mandatory Critical Infrastructure Protection (CIP) standards and financial incentives for implementation of the evolving National Institute of Standards and Technology (NIST) Framework Approach.
2. Payment of financial incentives should be dependent upon real-world demonstrations and tests of improved cybersecurity capabilities conducted by

parties outside the control of the utility – not a simple paperwork audit or internally-directed testing by employees of the incentivized utility.

BACKGROUND

On June 18, 2020 the Commission staff published a White Paper discussing a potential new framework for providing transmission incentives to utilities for cybersecurity investments. The Commission accepted comments from interested parties including Resilient Societies. We reiterate the primary points of our filing with these positions:

- Resilient Societies supports adoption of the National Institute of Standards and Technology (NIST) Framework as a supplement to the mandatory CIP Reliability Standards framework for cyber protection of the BPS.
- Resilient Societies does not support financial incentives for CIP Reliability Standards compliance, because we assess the CIP standards to exclude critical assets, including so-called "Low Impact" assets that are routinely targeted by foreign adversaries, including distribution system assets and vendor-managed software and firmware that can enable cyber-adversary takeover of critical grid assets.
- Resilient Societies does not support presumptions for rate of return adders based on CIP reliability standards that, overall, do not provide adequate protections from adversary cyber-attack capabilities.
- Incentives should be based on discernable performance metrics that can be empirically tested, without any presumptions that CIP standard compliance merits rate of return enhancements.

- Resilient Societies supports granting incentives based on the NIST Framework if utilities are willing to subject their networks to examination by third-party auditors ("Red Teaming" or "Penetration Testing") and if the results of outside audits are promptly and publicly disclosed after any vulnerabilities have been remedied.
- Resilient Societies supports incentives to protect corporate systems, and distribution assets outside the BPS, and financial aid to state utility commissions to strengthen cyber protection of the distribution grid.

While we recognize that at the time the CIP standards were developed the NIST Cybersecurity Framework was unavailable, in the interim Executive Order 13636 "Improving Critical Infrastructure Cybersecurity", released on February 12, 2013, charged NIST "to work with the private sector to identify existing voluntary consensus standards and industry best practices and build them into a Cybersecurity Framework."[1] It is our opinion that NIST has done an outstanding job of working with a broad spectrum of industries to generate "Best Practices" which would greatly improve the resiliency of the BPS.

Since the submission of our previous comments, major events have occurred: a) the Texas Deep Freeze in February which nearly caused a collapse of the ERCOT system; and b) two major cyberattacks in the US: SolarWinds[2] and Microsoft Exchange[3]. As to the former, the failure of Texas state regulatory system to prevent one of the largest blackouts in US history shows the absurdity of relying on plans alone to forestall a disaster. Although the Texas PUC

[1] https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636
[2] https://us-cert.cisa.gov/ncas/alerts/aa20-352a
[3] https://us-cert.cisa.gov/ncas/current-activity/2021/03/03/cisa-issues-emergency-directive-and-alert-microsoft-exchange

requires electric power generators to have a "severely cold weather" emergency plan[4], there are no requirements for the plan to be shown effective. As to the SolarWinds and Microsoft Exchange attacks, it is unknown whether these attacks affected the BPS. However, there are two things of which we can be certain:

1. Without a change in cybersecurity enforcement and incentives, consumers, businesses, investors and state regulators will be denied knowledge of their exposure to blackouts from vulnerabilities due to unreasonable use of CEII designations; and
2. If cybersecurity vulnerabilities not covered by the CIP standards are discovered, it will take months — if not years — for the CIP standards to catch up.

Finally, we trust both FERC and the North American Electric Reliability Corporation (NERC) realize that the SolarWinds attack came to light – and federal government victims first learned that they had been attacked -- due to a private cybersecurity firm, FireEye, publicly announcing its presence.[5] Had the SolarWinds attack been solely upon electric utilities, it is possible and perhaps likely that a concealment would have been attempted by the electric utility industry and the cybersecurity vulnerabilities would have been more slowly remedied, if at all.

GAPS IN CIP STANDARD SYSTEM

Because the current CIP standards were developed under a consensus-based system at NERC, this system generally suffers from these gaps and shortcomings:

---

[4] https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=16&pt=2&ch=25&rl=53

[5] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

1. The CIP explicitly exclude "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters."
2. The CIP are narrow in scope due to a time limit in the definition of BES Cyber Assets: "BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise."
3. CIP artificially separates the BES into High, Medium, and Low tiers based on power level with no thought to interconnectedness or vulnerability.
4. Compliance audits, which are performed by NERC regional entities, are infrequent and often have little or no repercussions for violators due to liberal use of the "Find, Fix, Track and Report" and "Compliance Exception" wavier processes.
5. The CIP have an opaque enforcement process because nearly all violations are classified as Critical Energy Infrastructure Information (CEII).
6. The timeline for updated CIP standards is many times longer than the development timeline of new threats.
7. Continued sole use of CIP Standards will lead to the "balkanization" of the nation's electric grid in terms of cybersecurity posture. This will occur in two ways: 1) geographically, as the state PUC regulated portions of the grid will opt for the NIST Cybersecurity Framework[6] which they can apply to multiple industries; and 2) between industries, as different regulators adopt differing standards. For example, National Grid, which operates utilities in multiple sectors, illustrates the latter point

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r4.pdf

in this response to a NIST survey:

"National Grid sees the greatest challenge in developing a cross-sector standards-based Framework as the harmonization of existing approaches to compliance within different sectors, whilst still leveraging the people, processes and technologies deployed. National Grid has both electric and gas assets within our footprint. Each of these sectors adopts differing and incongruent approaches to cybersecurity. Electric utilities take a prescriptive, rules-based, approach to cybersecurity in the form of mandatory NERC Critical Infrastructure Protection ("CIP") standards. Gas utilities are voluntary and principle-based with the adoption of the TSA Pipeline Security Guidelines. Finally, DHS takes a hybrid approach with the Chemical Facility Anti-Terrorism Standards. With operational cybersecurity standards alone, National Grid has three different approaches to cybersecurity with very little similarity in approach. Because of the inherent differences between industries, a principles-based framework would be more beneficial than a rules-based framework."[7]

ADVANTAGES OF NIST CYBERSECURITY FRAMEWORK

Although we recognize a direct comparison of CIP Standards to the NIST Cybersecurity Framework is akin to comparing apples and oranges[8], there are many features of the NIST Cybersecurity Framework which we believe would greatly improve the cybersecurity posture of the BPS. The NIST Cybersecurity Framework would have these advantages as a supplement to the CIP standards system:

[7] https://www.nist.gov/system/files/documents/2017/06/06/040813_national_grid.pdf
[8] Docket No. RM20-12-000 Comments of Christopher and Conway

1. Nationally-recognized standard framework which is also internationally recognized through ISO 2700x processes.
2. Incorporates “Best Practices” across numerous industries.
3. Requires senior management support.
4. Will treat BPS as part of a holistic energy network including fuel supply systems and telecommunications.
5. Provides ability to seamlessly mesh with distribution grid and other energy systems utilizing NIST Cybersecurity Framework.
6. Provides much larger pool of potential standard implementers and compliance monitors.
7. Ability to respond to emerging threats much more quickly.

NIST FRAMEWORK APPROACH

Resilient Societies supports incentives in tariff treatment for implementing security controls included in the NIST Framework (NIST Framework Approach). We applaud Commission staff for identifying five types of security controls included in the NIST Framework that may be considered for incentives under the NIST Framework approach and are disappointed that only one is being forwarded for implementation at this time. However, given that “automated and continuous monitoring” could be used for the primary CIP weakness of “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters,” we support the use of this particular security control of the NIST Cybersecurity Framework and anticipate seeing more controls proposed in the future.

CRITERIA FOR AWARD OF FINANCIAL INCENTIVES

Resilient Societies proposes a high bar be set to merit financial incentives. Unlike CIP Standards, which are deemed to be satisfied based on paper review alone, we propose that award of either type of financial incentive (ROE Adder or Regulatory Incentive) depend on successful demonstration of cybersecurity protections in a real-world environment. It goes without saying that performing experiments on an operational portion of the grid should only be done with the utmost care; however, there are alternatives. For example, Southern Company has developed its own simulation laboratory (Figure 1)[9] which would be ideal for evaluating the efficacy of cyber-defense features. In addition, there are national facilities such as the RADICS testbed at Plum Island (Figure 2)[10] and the Idaho National Laboratory (INL) Electric Grid Testbed (Figure 3)[11] which could be used for larger scale demonstrations. Our nation has decades of experience using "Hardware in the Loop" testbeds such as these to evaluate software changes in industrial control systems, and recommend this same approach be utilized for evaluating BPS cyber-defenses.

[9] https://www.naspi.org/sites/default/files/2020-11/03_socompany_black_grid_vis_20201103.pdf
[10] https://www.darpa.mil/news-events/2021-02-23
[11] https://inl.gov/critical-infrastructure-protection/#power-systems

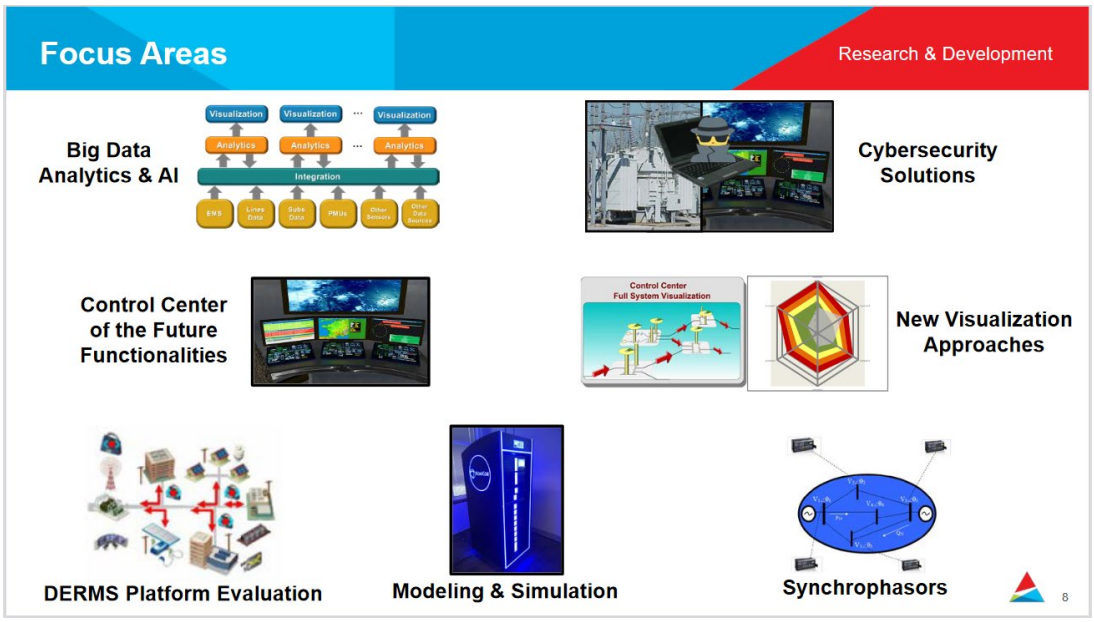


Figure 1. Southern Company's Schatz Grid Visualization & Analytics Center (SGVAC)

Figure 2. RADICS Substations-In-A-Box crankpath being restored as part of the exercise at Plum Island, NY in October 2020

Figure 3. INL has the most instrumented grid in the nation and can validate models at full scale

BROADER USE OF CYBER RANGES

Resilient Societies further proposes that FERC direct NERC to greatly increase their use of cyber ranges and realistic cyberattack scenarios, including those listed above, to harden the BPS. There can be no doubt that the US is in a cyberwar with our foreign adversaries as well as mercenaries who act as the pirates of the internet. Therefore, FERC and NERC need to take a military mindset in which field exercises and realistic engagements are required to defeat the enemy. Lessons learned from such exercises could benefit the BPS much more than fiddling with CIP standards. FERC and NERC should take advantage of the recently passed 2021 NDAA (Title XVII)[12] and partner with National Guard cyber units to act as "Red Team" participants.

[12] https://www.congress.gov/bill/116th-congress/house-bill/6395/text

NERC is to be commended for their biannual GRIDEX exercise. It is without a doubt a valuable large scale exercise emphasizing command and control. By comparison, our proposal is much smaller and more focused in scope. In the near future, we would hope to see an initiative by NERC to partner with DARPA and/or INL to make extensive use of their cyber ranges and require all NERC members to participate in a focused cyberattack exercise on an annual basis.

RED TEAM EXERCISES

In the August 2020 US Senate Energy Committee "Hearing to Examine Efforts to Improve Cybersecurity for the Energy Sector"[13], Senator Manchin repeatedly stressed the need for "Red Team" and penetration testing to interrogate the security of electricity networks. We wholeheartedly agree. Earlier, we said that penetration testing of operating electricity systems needed to be done with utmost care. While this is true, it does not mean it is impossible. In fact, in 2016 the Snohomish County Public Utility District (Water & Power) invited the Washington State National Guard to perform a cyberattack exercise. Although the National Guard "Red Team" took control of the Snohomish PUD network, "the two sides used a nearly identical test lab network to preserve service-delivery during the two-week test." [14] Importantly, lessons learned from this successful third party penetration testing resulted in an augmented mission for the State of Washington National Guard, improvements in cybersecurity

[13] https://www.energy.senate.gov/hearings/2020/8/full-committee-hearing-to-examine-federal-and-industry-efforts-to-improve-cybersecurity-for-the-energy-sector

[14] https://www.usnews.com/news/articles/2016-09-23/is-the-energy-grid-in-danger

elsewhere in Washington State, and support for National Guard cybersecurity missions now applicable for all 50 states.[15]

For decades, the U.S. Nuclear Regulatory Commission (NRC) has performed regular inspections of licensee facilities using expert physical and cybersecurity attack capabilities—commonly called "Red Teams"—that add practical understanding of how various security plans, training, and adaptability work in practice. The interaction of Red Team attack-versus-plant defense yields insight to regulators and also to plant owners and operators. The NRC shares "lessons learned" with other operator-owner licensees. These Red Team exercises have arguably greater credibility and merit than the "paper plans" and "paper trails" of utilities not testing in the field.

Dr. George H. Baker, a former director of the Foundation for Resilient Societies, has reviewed records of a contractor conducting "Balanced Survivability Assessments" of vulnerabilities of critical national and infrastructure sites in the period 1987-2016. His overview is as follows:

> *BSA team subject matter experts first took steps to understand the entire system. The assessments focused on mission survivability with an emphasis on identifying single point vulnerabilities (SPVs). The team had experts on electric power, physical security, cyber security, kinetic kill effects, electromagnetic security, and special operations/sabotage. Experts' experience covered all types of systems and all hazards. All team members had the highest available security clearances. Assessments involved 2-3 weeks*

[15] The National Defense Authorization Act for FY2021, which entered into force on January 1, 2021 has multiple programs that support utilization of the state National Guards to support critical infrastructure cybersecurity. See Public Law 116-283, for example, sections 1621, 1623 1627, 1628. The state National Guards might provide 3rd party, independent field testing of FERC-jurisdictional utility initiatives, helping to support identification of effective or defective cybersecurity enhancing utility programs. Indirectly, lessons learned from National Guard cyber-testing experiences could improve FERC criteria for determining which "best practices" programs should qualify for FERC approvable financial incentives.

on site plus post-site analysis. Findings were provided only to the customer at a classification level directed by the customer.

Past facilities assessed include major hydroelectric dams, national command/control/data centers, global communication sites, satellite control facilities, airfields, ports, manufacturing sites, and medical research facilities. Assessments have resulted in major improvements in system survivability. Such assessments would have major benefit in assuring the survivability of critical electric power grid facilities to cyber attacks and/or all-hazards.

Resilient Societies urges FERC to develop a family of field-based, merit-based assessments of cybersecurity protection capabilities and projected requirements. Voluntary "best practices" programs should utilize third party-validated, independent metric-supported assessments as key elements to reward cybersecurity best practices initiatives.

RISK ASSESSMENTS BY THIRD PARTIES

The NOPR proposes cost recovery for "risk assessments by third parties." We support this provision because it would allow the use of not only "Red Teams" but also "penetration testing". Over the last several years a veritable cottage industry of cybersecurity professionals has sprung up. We encourage NERC and its members to take advantage of these resources and urge FERC to include such costs in incentive payments. Once again, we urge both entities to set the bar high, and not settle for merely a vulnerability scan.

PUBLIC DISCLOSURE

As we have stated in previous filings[16], we strongly disagree with FERC's broad extension of CEII to prevent public disclosure of registered entity security vulnerabilities that have been remedied before disclosure would occur. We find this practice of concealment abusive to the public interest and inconsistent with the NOPR's proposed financial incentives for "best practices." There is no question the United States faces a number of adversaries – both nation states and mercenaries – who would delight at having unfettered access to truly sensitive information. However, the fact that the BPS is generally vulnerable to cyberattack should not be considered sensitive information. To assert that ratepayers, investors and the American public in general has no "Need to Know" about remedied vulnerabilities is disingenuous at best. To the contrary, should incentives be paid out, this fact should incentivize other entities to participate. No incentives should be paid out unless accompanied by the following public information:

- Identity of the incentivized entity
- Amount of the incentive
- What type of cybersecurity demonstration merited the incentive
- A general description of the enhancement made before or after the cybersecurity demonstration (e.g., NIST Cybersecurity Framework Category)

CIP STANDARDS: THE MAGINOT LINE OF CYBERSECURITY

Any student of Europe 20th century history knows the story of the Maginot Line: a perfect defense for World War I which was rendered useless by the technologies of WW II. The

[16] https://elibrary.ferc.gov/eLibrary/docinfo?document_id=14814927

French of the 1930s suffered from what would now be called a "failure of imagination." Invoking the theme once again that the BPS is in the midst of a war, we implore FERC and NERC to recall the lesson of the Maginot Line. The contrast between the ponderous CIP standards, initiated in 2006 and slowly, incrementally updated since then, to the quickness and agility of today's cyber enemy is remarkable. We have already pointed out numerous deficiencies with the CIP standards above. We have no doubt there are many others, and further assert that deficiencies will increase with time. We hope that this NOPR is followed by more in the future which would accelerate the ability of the BPS to behave in a more agile and timely manner in response to evolving cyber threats—and to avoid the fate of the Maginot Line.

COMMISSIONER COMMENTS

Chairman Glick and Commissioner (and former chairman) Danly pose two very important questions in their comments related to this NOPR:

1. Can the Commission better address cybersecurity threats by directing NERC to expand its critical infrastructure protection (CIP) standards to require some or all of the investments contemplated in this NOPR?
2. Are public utilities not adopting the contemplated measures because the existing financial incentives are insufficient?

Our answer to both Questions 1 and 2 is "No" under current policies of the Commission. As to Question 1, there is little public evidence that the present CIP Standards materially improve the cyber posture of the BPS. The risk that utilities will be publicly exposed as having imprudent cybersecurity measures is likely a stronger motivator. As long as penalties for CIP standards violations are kept at a minimal level and out of the public view via the CEII process,

there are few incentives for regulated utilities to invest in cybersecurity beyond their needs to protect financial viability and marketplace reputation. Similarly, our answer to Question 2 is not that financial incentives are insufficient but rather that penalties—including the risk of public exposure—are insufficient to motivate the desired behavior.

We suggest it would be instructive to look at what is occurring in private industry in response to the cyber arms race. After suffering a massive cyberattack from China, Google initiated the Vulnerability Reward Program[17] to encourage hackers to attack their products. Google made a business decision that it was better to discover vulnerabilities and patch them before adversaries had the chance to launch an attack. Several other companies have followed suit, including Microsoft[18], Facebook[19] and GitHub[20]. Even the Department of Defense has begun to participate in sponsored hacking activities, beginning with "Hack the Pentagon" in 2016 and most recently "Hack the Army 3.0".[21]

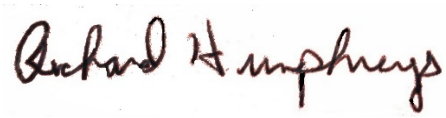
We suggest FERC survey the cyber "Best Practices" that successful, profit motivated companies have already taken rather than adding more features to the Maginot Line. Until the motivation to get serious about cybersecurity comes from within the utility industry, the addition of more rules is likely a poor use of time and resources.

[17] https://www.google.com/about/appsecurity/reward-program/
[18] https://www.microsoft.com/en-us/msrc/bounty
[19] https://www.facebook.com/whitehat
[20] https://bounty.github.com/
[21] https://www.army.mil/article/240719/hack_the_army_3_0_furthers_innovative_bug_bounty_program_to_defend_networks_data

CONCLUSION

FERC, NERC and its Regional Entities, regulated utilities, and electricity consumers now have fifteen years of experience in standard-setting, compliance, and auditing under the mandatory CIP standards system. The CIP standards have set a valuable baseline for BPS cybersecurity but are slow to adapt to new threats. A fundamental weakness of the CIP system is difficulty in achieving cost recovery for utilities. The proposed NOPR would augment the baseline CIP standards system with the more adaptable NIST Framework Approach. Because a cost recovery mechanism is built into the proposed rule, utilities could act more quicky in addressing cyber-threats while being confident that they will not incur unreimbursed charges. We support the approach outlined in the NOPR.

Respectfully submitted by:



Richard H. Humphreys, Director
richardh@resilientsocieties.org

William R. Harris, Director Emeritus
williamh@resilientsocieties.org

for the
Foundation for Resilient Societies
24 Front Street, Suite 203
Exeter, NH 03833
www.resilientsocieties.org