UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Security Investments for Energy Infrastructure Technical Conference	Docket No. AD19-12-000

POST-TECHNICAL CONFERENCE COMMENTS OF THE TRANSMISSION ACCESS POLICY STUDY GROUP

The Transmission Access Policy Study Group ("TAPS") appreciates the opportunity to respond to the Commission's April 25, 2019 Notice Inviting Post-Technical Conference Comments regarding the March 28, 2019, *Security Investments for Energy Infrastructure* technical conference.[1] TAPS supports the goal of continuing to secure the grid against physical and cyber threats. TAPS comments on the following two issues:

- Mitigation measures should be risk-based, with smaller utilities making security investments commensurate with the risk they pose to the grid.
- Given that utilities with cost-of-service rates are able to recover the costs of any prudent security investments, it is neither necessary nor appropriate to grant them financial incentives for such investments.

INTEREST OF TAPS

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states promoting open and non-discriminatory transmission access.[2] Representing

[1]Notice Inviting Post-Technical Conference Comments (Apr. 25, 2019), eLibrary No. 20190425-3008 ("Notice"). *See also* Transcript of Technical Conference (Apr. 26, 2019), eLibrary No. 20190426-4001 ("Tr."); Supplemental Notice of Technical Conference (Mar. 21, 2019), eLibrary No. 20190321-3136 ("Supplemental Notice").

[2] David Geschwind, Southern Minnesota Municipal Power Agency, chairs the TAPS Board. Jane

entities entirely or predominantly dependent on transmission facilities owned and controlled by others, TAPS has long recognized the need for reliable and secure transmission infrastructure that enables TAPS members to serve their load affordably. As TDUs, TAPS members make investments to secure their own assets and pay, through transmission rates, for investments made by other utilities to improve their transmission facilities security. TAPS supports cost-effective, risk-informed security investments. TAPS has therefore participated actively in numerous Commission proceedings concerning transmission planning, pricing, and incentives policies. In addition, many TAPS members participate in the development of and are subject to compliance with North American Electric Reliability Corporation ("NERC") reliability standards.

Communications regarding these proceedings should be directed to:

John Twitty
Executive Director
TRANSMISSION ACCESS POLICY STUDY GROUP
PO Box 14364
Springfield, MO 65814
(417) 838-8576
Email: jtwitty@tapsgroup.org

Cynthia S. Bogorad
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000
Email: cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

Cirrincione, Northern California Power Agency, is TAPS Vice Chair. John Twitty is TAPS Executive Director.

COMMENTS

I. MITIGATING SECURITY THREATS TO THE GRID SHOULD BE RISK-BASED.[3]

Utilities have a variety of tools available to mitigate the physical and cyber security threats to our electric grid. Given the range of threats, each utility must develop mitigation strategies that are tailored to the specific risks that it faces. For example, different security measures are appropriate for a regional transmission organization's control center than for a single generating station. Utilities, therefore, should consider the risks they face and pose to the grid, and adopt appropriate security measures commensurate with those risks. That risk-based approach to security is consistent with the NERC Critical Infrastructure Protection ("CIP") standards,[4] and with the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework.[5]

Claims that small utilities "don't have the wherewithal to be able to invest in all these kinds of activities that the larger companies are,"[6] wrongly ignores that fundamental risk-based principle. Small entities should *not* be making the same level of investment as large ones given the lower risk small entities pose to the grid. Rather, it is appropriate for them to focus on investments and security practices commensurate with the lower risk that those entities pose to the grid. And there is evidence that they are

[3] This section responds to Panel I, Questions 6-10 (Mitigation: Strategies and Best Practices) from the March 21, 2019 Supplemental Notice. *See* April 25 Notice ("Commenters should organize responses consistent with the numbering of the questions in the Supplemental Notices.")

[4] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, P 35, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016). ("We intend that NERC's proposed modifications will be designed to address the risk posed by the assets being protected in accordance with the risk-based approach reflected in the CIP version 5 Standards, *i.e.*, the modifications to address Low Impact BES Cyber Systems may be less stringent than the provisions that apply to Medium and High Impact Cyber Systems – commensurate with the risk.")

[5] *See* U.S. Dept. of Commerce, Nat'l Inst. of Standards & Tech., http://www.nist.gov/cyberframework/ (last visited May 23, 2019).

[6] *See* Tr. at 79-80 (Nicholas Akins).

doing so.[7] Such risk-informed approaches to security are appropriate and cost effective, and warrant continued Commission support.

In addition, there are opportunities for the federal government to promote infrastructure security for small utilities through grants or other programs. For example, the Department of Energy's ("DOE") cooperation agreement with the American Public Power Association has resulted in tools that public power utilities can use to increase the security of their cyber systems.[8] Those tools, such as the cyber security scorecard, have "pa[id] big dividends in promoting infrastructure security even where the dollars are not spent on specific facilities."[9] Similarly, several panelists at the technical conference discussed the value of the DOE's Cybersecurity Risk Information Sharing Program ("CRISP") while bemoaning that it is inaccessible to all but the largest of utilities.[10] Expanding CRISP or its functionality to more utilities is another example of an investment that the federal government could make that could improve security.[11]

Small utilities take measures to secure their assets so they can keep the lights on in their communities. Both through their own efforts and through partnership with others, small entities can—and do—make investments and implement security controls that are appropriate for their size and the risks they face.

[7] *See* Am. Pub. Power Ass'n & Nat'l Rural Elec. Coop. Ass'n., *Managing Cyber Supply Chain Risk-Best Practices for Small Entities* 10 (2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Managing%20Cyber%20Supply%20Chain%20Risk.pdf; Tr. at 134:21-135:13 (Kevin Wailes) (describing efforts of small utilities).

[8] *See* Written Statement of Kevin Wailes, Lincoln Electric System 6 (Mar. 26, 2019), eLibrary No. 20190402-4009.

[9] Tr. at 135:3-6 (Kevin Wailes).

[10] *See, e.g.,* Tr. at 128:24-129:7 (Nicholas Brown), 157:1-7 (Christopher Crane), 171:7-14 (Kevin Wailes), 188: 12-189:7 (Commissioner Glick).

[11] *See id.* at 171:7-9 (Kevin Wailes) (suggesting that programs like CRISP may be a national prerogative that should be funded as part of defending the nation).

II. FINANCIAL INCENTIVES FOR SECURITY INVESTMENTS ARE NEITHER NECESSARY NOR APPROPRIATE.[12]

TAPS does not support financial incentives to promote security investments for utilities with cost-of-service rates. As an initial matter, utilities are already required to take certain security measures in compliance with NERC reliability standards. Consistent with the Commission's "longstanding policy that incentives should only be awarded to induce voluntary conduct,"[13] incentives are not needed for investments made in compliance with those mandatory standards.

Even for security investments made above and beyond what is required by mandatory standards, financial incentives are unnecessary for two reasons: (1) the Commission's existing cost recovery policies adequately incentivize such investments; and (2) adding further incentives would invite gold-plating.

First, as Chairman Chatterjee noted, the Commission "has been very accommodating in providing a number of mechanisms for utilities to recover the costs of their prudently incurred security expenditures."[14] The widespread adoption of formula rates for transmission assets, combined with the Commission's "presum[ption] that all expenditures are prudent,"[15] significantly reduces the risk that transmission owners will not recover costs related to improving grid reliability and security beyond what is required by mandatory standards.[16] In fact, Commissioner Glick's conclusion at the end

[12] This section responds to Panel II, Questions 9-13 (Financial Incentives).

[13] *Cal. Pub. Util. Comm'n v. FERC*, 879 F.3d 996, 978 (9th Cir. 2018).

[14] Tr. at 151:4-7.

[15] *Potomac-Appalachian Transmission Highline, LLC*, 158 FERC ¶ 61,050, P 100 (2017).

[16] Section 215A of the Federal Power Act provides a mechanism for owners, operators or users of critical electric infrastructure to recover prudently incurred costs to comply with an emergency order to the extent they are not recovered through regulated rates. 16 U.S.C. § 824o-1(b)(6).

of the March 28 conference was that "cost recovery at the state or federal level really isn't a barrier to utilities doing what they need to do to protect . . . from physical or cyberattacks."[17]

Investors have confirmed that investing in grid reliability is a good deal. Nick Akins, CEO of American Electric Power, stated that investments in resiliency and reliability of the grid, are "really probably one of [the] least risky investments we can make."[18] Edison Electric Institute ("EEI") estimates that electric utilities have invested $285 billion in transmission and distribution since 2012 to harden the grid and make it more resilient.[19] That trend will continue into the future, with EEI estimating that "about a quarter of electric company transmission spending through at least 2021 is expected to be devoted to improving resilience and security, as well as to integrating advanced technologies."[20]

In short, investors have been investing and will continue to invest heavily in transmission projects that improve security—above and beyond what is required by mandatory standards—because the Commission's cost recovery policies make such projects attractive, low-risk investments.

[17] Tr. at 187:22-24; *see also id.* at 78:16-19 (Nicholas Akins) (regulators typically allow recovery of costs associated with resiliency and reliability of the grid); *id.* at 151:13-16 (Christopher Crane) (Exelon's six utilities "have not experienced any issues with recovery on the prudent investments around the physical and cybersecurity.").

[18] *Id.* at 78:16-19 (Nicholas Akins).

[19] Edison Elec. Inst., *Smarter Energy Infrastructure: The Critical Role and Value of Electric Transmission* 3 (2018), http://www.eei.org/issuesandpolicy/transmission/Documents/2018%20Smarter%20Energy%20Infrastructure%20The%20Critical%20Role%20and%20Value%20of%20Electric%20Transmission.pdf.

[20] *Id.* at 5.

The second reason TAPS does not support incentives for improving security is that doing so would invite utilities to gold-plate their systems.[21] This is especially true for security projects not selected through an open and transparent transmission planning process. More than a decade ago, the Commission acknowledged that transmission owners could not be relied on to expand the grid in a not unduly discriminatory manner, and thus implemented Order 890's transmission planning requirements.[22] In Order 1000, the Commission relied on evidence of unduly discriminatory and preferential practices in the transmission planning process to adopt additional reforms.[23] Yet transmission owners continue to make massive investments—in some cases more than half of their transmission investment—on "supplemental" or "asset management" projects that are not subject any transmission planning process and approved only by utility executives.[24] Much of that self-approved transmission investment is for reliability and security projects.[25] Particularly given the limited scrutiny of the need for and cost-effectiveness of such projects, additional incentives all but invite a profit-maximizing transmission owner to enhance their bottom line by gold-plating such projects.[26]

[21] Tr. at 156:22-25 (Commissioner Chatterjee seeking input on the balance between appropriate security investments while "not gold-plating the system.").

[22] *Preventing Undue Discrimination and Preference in Transmission Service*, Order No. 890, 118 FERC ¶ 61,119, PP 39-40, *order on reh'g and clarification*, Order No. 890-A, 121 FERC ¶ 61,297 (2007), *order on reh'g*, Order No. 890-B, 123 FERC ¶ 61,299 (2008), *order on reh'g and clarification*, Order No. 890-C, 126 FERC ¶ 61,228, *order on clarification*, Order No. 890-D, 129 FERC ¶ 61,126 (2009).

[23] *Transmission Planning and Cost Allocation by Transmission Owning and Operating Public Utilities*, Order No. 1000, 136 FERC ¶ 61,051, PP 58-59 (2011), *reh'g denied*, Order No. 1000-A, 139 FERC ¶ 61,132, *on reh'g*, Order No. 1000-B, 141 FERC ¶ 61,044 (2012), *review denied sub nom. S.C. Pub. Serv. Auth. v. FERC*, 762 F.3d 41 (D.C. Cir. 2014) (per curiam), *reh'g en banc denied*, No. 12-1232 (D.C. Cir. Oct. 17, 2014).

[24] *See, e.g., Cal. Pub. Utils. Comm'n v. Pac. Gas & Elec. Co.*, 164 FERC ¶ 61,161 (2018) (allowing 60% of Pacific Gas and Electric Company's ("PG&E") capital transmission spending authorized through a self-approval process that involves only PG&E's Chief Financial Officer and Project Managers).

[25] *Id.* P 30.

[26] Exelon CEO Christopher Crane stated that "it's not our intent in our transmission planning process that

None of the panelists indicated that transmission owners are failing to make adequate security investments; in fact, all the evidence suggests the contrary: the Commission's current policies *already* incent security projects that go above and beyond the mandatory standards. Adding unnecessary incentives will simply result in unjust and unreasonable rates.

CONCLUSION

As the Commission and the DOE consider what steps should be taken to further secure the nation's energy infrastructure against physical and cyber threats, they should adopt risk-based approaches, consistent with the approaches of NERC CIP standards and the NIST cyber security framework. Additionally, the Commission should not adopt financial incentives for transmission owners to invest above and beyond what is required by mandatory standards, because such incentives are unnecessary to attract investment and would invite gold-plating.

---

we utilize to gold-plate, but to ensure we're doing everything to remove vulnerabilities." Tr. at 157:1-4. But there is no apparent mechanism, other than the utility's "intent" to prevent gold-plating. In contrast, utilities continue to tell their investors that growing transmission investment is a key contributor to growth in earnings per share. *See* Eversource Energy, 2018 Year-End Results Investor Call 13, 26 (Feb. 21, 2019), available at https://www.eversource.com/content/docs/default-source/investors/2018-q4-and-year-end-results.pdf?sfvrsn=dd0ecb62_0; FirstEnergy, Quarterly Highlights – Q4 2018 Earnings 5,7 (Feb. 20, 2019), available at https://investors.firstenergycorp.com/Cache/1500117495.PDF?O=PDF&T=&Y=&D=&FID=1500117495&iid=4056944; Am. Elec. Power, 2018 Annual Report 18 (2019), available at https://aep.com/Assets/docs/investors/AnnualReportsProxies/docs/18annrep/2018AnnualReportAppendixAtoProxy.pdf.

Respectfully submitted,

/s/ Cynthia S. Bogorad

Cynthia S. Bogorad
Latif M. Nurani

Attorneys for Transmission Access Policy Study Group

Law Offices of:
Spiegel & McDiarmid LLP
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 879-4000

May 28, 2019