UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives	Docket No. RM21-3-000

COMMENTS OF
TRANSMISSION ACCESS POLICY STUDY GROUP

The Transmission Access Policy Study Group ("TAPS") appreciates the opportunity to comment on the Commission's December 17, 2020 Notice of Proposed Rulemaking ("NOPR").[1]

TAPS shares the Commission's concerns about the challenges of addressing fast-evolving cyber challenges through prescriptive, inflexible North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Standards. But the NOPR's proposal is not an effective or cost-efficient way of addressing those concerns. Instead, the Commission can best address the cybersecurity threats by focusing on offering non-financial incentives and supporting NERC's efforts to effectively utilize tools other than Reliability Standards to mitigate evolving risks. In these comments, TAPS explains:

- The NOPR has not satisfied the requirements for granting incentives under Section 205. *See* Section II.A.
- Public utilities already have ample financial incentive to make prudent cybersecurity investments; the proposed incentives will increase consumer costs without ensuring that consumers receive commensurate security benefits. *See* Section II.B.

[1] *Cybersecurity Incentives*, 173 FERC ¶ 61,240 (2020) ("NOPR").

- The proposed NERC CIP Incentives Approach is not likely to materially enhance security in all circumstances, so the Commission should *not* grant a rebuttable presumption that such investments will benefit consumers. *See* Section II.C.

- The National Institute of Standards and Technology ("NIST") Framework Approach does not adequately define what types of investments will qualify for an incentive, and the NOPR's examples will not always produce consumer benefits. *See* Section II.D.

- The Commission should not grant incentives for cybersecurity investments in generators with market-based rate authority or in corporate IT systems. *See* Section II.E.

- The proposal lacks sufficient verification mechanisms and meaningful consequences for non-compliance. *See* Section II.F.

- The proposal does not provide adequate time for customers to obtain un-redacted incentive applications, meaningfully evaluate a utility's request, and submit comments to the Commission. *See* Section II.G.

- The Commission should *not* mandate the "best practices" proposed to be incented in this NOPR. *See* Section II.H.

I. INTEREST OF TAPS

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

---

[2] David Geschwind, Southern Minnesota Municipal Power Agency, chairs the TAPS Board. Jane Cirrincione, Northern California Power Agency, is TAPS Vice Chair. Terry Huval is TAPS Executive Director.

In addition, many TAPS members participate in the development of and are subject to compliance with NERC reliability standards, including the CIP standards. In addition to participating at NERC and before the Commission on policy matters related to cybersecurity, TAPS has participated actively in numerous Commission proceedings concerning transmission incentive policies, including those underlying Order 679,[3] the 2012 Policy Statement,[4] the 2019 Notice of Inquiry on transmission incentives,[5] and the Commission's pending Notice of Proposed Rulemaking in Docket No. RM20-10.[6] TAPS has supported use of risk-reducing incentives, rather than cost-increasing incentives.

Communications regarding these proceedings should be directed to:

Terry J. Huval
Executive Director
TRANSMISSION ACCESS POLICY STUDY GROUP
P.O. Box 60551
Lafayette, LA 70596
(337) 278-0306
Email: thuval@tapsgroup.org

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

II. COMMENTS

A. The NOPR has not satisfied the requirements for granting incentives under Section 205.

Section 205 of Federal Power Act ("FPA"), 16 U.S.C. § 824d, requires that rates be just and reasonable. The Commission has asserted its authority to depart from

---

[3] *Promoting Transmission Investment through Pricing Reform*, Order No. 679, 116 FERC ¶ 61,057, *on reh'g*, Order No. 679-A, 117 FERC ¶ 61,345 (2006), *clarified*, 119 FERC ¶ 61,062 (2007).

[4] *Promoting Transmission Investment Through Pricing Reform*, 141 FERC ¶ 61,129 (2012).

[5] *Inquiry Regarding the Commn's Elec. Transmission Incentives Pol'y*, 166 FERC ¶ 61,208 (2019).

[6] *Elec. Transmission Incentives Pol'y Under Section 219 of the Fed. Power Act*, 170 FERC ¶ 61,204, *errata notice*, 171 FERC ¶ 61,072 (2020).

traditional cost-of-service principles and to grant public utilities incentive rate treatment under Section 205.[7] The Commission has also articulated in its Incentive Policy Statement key principles that must be upheld to ensure an incentive rate is just and reasonable.[8] The NOPR cites to the Incentive Policy Statement, but does not explain how the proposal complies with that policy statement; in fact, the NOPR's proposal departs from three of the key principles.

First, the Incentive Policy Statement requires that there be a "correlation between the incentive and the result to be induced."[9] That is, the Federal Power Act requires an incentive to be "in fact needed and . . . no more than is needed, for the purpose."[10] The NOPR does not satisfy that basic principle, because it has not demonstrated that additional financial incentives are needed to induce prudent cybersecurity investments. This issue is discussed further in Section II.B, below.

Second, the Incentive Policy Statement requires that incentive mechanisms "must be understood by all parties" and that the net "benefits to consumers must be quantifiable."[11] For an incentive rate to be just and reasonable, the Commission must identify an investment's benefits and demonstrate that those benefits outweigh the cost of

---

[7] *Incentive Ratemaking for Interstate Nat. Gas Pipelines, Oil Pipelines, & Elec. Utils.*, 61 FERC ¶ 61,168, at 61,594 (1992) ("Incentive Policy Statement").

[8] *Id.*

[9] *Id.* (citing *Pub. Serv. Comm'n for the State of N.Y. v. FPC*, 487 F.2d 1043 (D.C. Cir. 1973)*; City of Charlottesville, Va. v. FERC*, 661 F.2d 945 (D.C. Cir. 1981)).

[10] *City of Detroit v. FPC*, 230 F.2d 810, 817 (D.C. Cir. 1955); *see also Farmers Union Cent. Exch. v. FERC*,734 F.2d 1486, 1503 (D.C. Cir. 1984) (rejecting incentive rates because the Commission '"must see to it that the increase is in fact needed, and is no more than is needed, for the purpose."' (quoting *City of Detroit*, 230 F.2d at 817)). *Cf.*, *Hope Nat. Gas v. FPC*, 320 U.S. 591, 652-53 (1944) ("The function which an allowance for gas in the field should perform for society in such circumstances is to be enough and no more than enough to induce private enterprise completely and efficiently to utilize gas resources, to acquire for public service any available gas or gas rights and to deliver gas at a rate and for uses which will be in the future as well as in the present public interest.").

[11] Incentive Policy Statement at 61,590.

the incentive.[12] The NOPR does not satisfy these principles in four respects: (a) as discussed in Section II.C below, the NOPR's NERC CIP Incentives Approach fails to demonstrate any benefit to consumers; (b) as discussed in Section II.D below, the NOPR's NIST Framework Approach is not understandable because it does not clearly define the activities that would qualify for an incentive; (c) as discussed in Section II.E below, the NOPR is unclear on which investments in generation resources and non-Bulk Electric System ("BES") assets will qualify for incentives and how those investments will benefit consumers; and (d) as discussed in Section II.F below, the NOPR's proposed application process does not give customers a meaningful opportunity to evaluate and respond to any incentive requests.

Finally, the Incentive Policy Statement requires that incentives be symmetric: "opportunities for reward should be offset by a symmetric downside risk."[13] The NOPR does not satisfy that principle, because its lack of penalties for non-compliance eliminates any risk for utilities to comply. This issue is discussed further in Section II.G, below.

B. Financial incentives are not needed to induce prudent and appropriate cybersecurity investments.

1. Utilities are already making above-and-beyond cybersecurity investments, supported by existing cost-recovery mechanisms and non-financial incentives.

The NOPR lacks any evidence of the cybersecurity investments utilities are currently making that go above and beyond the CIP Standards. The NOPR assumes—

---

[12] *See Pub. Utils. Comm'n of Cal. v. FERC*, 367 F.3d 925, 929 (D.C. Cir. 2004); *see also id.* at 931 ("If the Commission wants to depart from this [cost-of-service] formula and offer additional incentives, it must carefully tailor them, lest it run afoul of the requirement that rates be 'just and reasonable.' Otherwise, the 'incentives' are nothing but windfalls.") (Rogers, J., concurring in part and dissenting in part).

[13] Incentive Policy Statement at 61,590.

without any analysis—that utilities are failing to make such above-and-beyond investments. Not only is that assumption unsupported, but it is also incorrect.

Utilities have told investors and state commissions that they are investing in cybersecurity beyond the minimum requirements; their trade associations have made similar public comments. EEI asserts that "standards provide a solid foundation for strengthening the industry's security posture. . . . [but] the industry's efforts are moving *beyond baseline standards*."[14] In a 2015 NIST Case Study, NIST reports that Exelon was already using the NIST Cybersecurity Framework and quotes an Exelon executive as saying, '"Compliance with regulations is an important baseline, but security requires that we go beyond the status quo to keep pace with the threat."'[15] And in the past six months, Ameren, National Grid, and others have reported on shareholder calls that they use the NIST Framework in addition to complying with the CIP Standards.[16] Other utilities have told state regulators that they are implementing the NIST Framework.[17]

---

[14] Edison Electric Institute, *Protecting the Energy Grid for Customers* 2 (Feb. 2021), https://www.eei.org/issuesandpolicy/Documents/Protecting_the_Energy_Grid.pdf (emphasis added).

[15] Exelon Corporation, *US Resilience Project - Best Practices in Cyber Supply Chain Risk Management*, NIST 10, https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Exelon-Case-Study.pdf (last visited Mar. 29, 2021) ("NIST U.S. Resilience Project").

[16] Ameren, *Leading the Way to a Sustainable Energy Future* (Feb. 2021), https://s21.q4cdn.com/448935352/files/doc_presentations/2021/02/Ameren-ESG-Investor-Deck-Feb-2021-FINAL.pdf; National Grid, *ESG Virtual Seminar –Transcript of Q&A Sessions* (Oct. 5, 2020), https://www nationalgrid.com/document/140526/download.

[17] *See e.g., Proceeding on Motion of the Comm'n as to the Rates, Charges, Rules & Regs. of N.Y. State Elec. & Gas Corp. for Elec. Serv.*, Case Nos. 19-E-0378 et al., Joint Proposal, Appx. O (AMI-2) at 46 (N.Y. Pub. Serv. Comm'n May 21, 2020) ("AVANGRID has implemented a formal Cyber Security Program (Program) and a Controls Framework based on industry standards of best practice to protect the confidentiality, integrity, availability and reliability of our cyber-infrastructure and its associated cyber-assets . . . .The Controls Framework creates a common language for identifying and implementing cybersecurity and privacy standards of best practice. Industry standards and best practice guidance used in the development and maintenance of the Controls Framework include, but are not limited to: - NIST Cybersecurity Framework [and other NIST publications]"); *Application of S. Cal. Edison Co. (U338E) for Authority to Increase its Authorized Revenues for Elec. Serv. In 2021, Among Other Things, And To Reflect That Increase In Rates*, No. A.19-09-013, Opening Brief of Southern California Edison Company (U 338-E), at 194, 196-97 (Pub. Utils. Comm'n of Cal. Sept. 11, 2020) (requesting to recover labor costs for

It is no surprise that utilities are making these above-and-beyond cybersecurity investments. The business case for doing so is strong: it is a low-risk investment[18] that is essential to maintaining the utility's reputational value[19] and continuity of service for its customers.[20]

And the Commission already provides ample financial mechanisms to induce utilities to make prudent cybersecurity investments. The Commission "has been very accommodating in providing a number of mechanisms for utilities to recover the costs of their prudently incurred security expenditures."[21] The Commission Staff White Paper notes the variety of actions the Commission has specifically taken to that end, including: widely adopting formula rates that flow through costs automatically; presuming all costs are prudent; allowing security costs in stated rates; and even granting a separate, security-related surcharge to recover costs.[22] This backdrop, along with comments from utilities

---

"staffing to support the National Institute of Standards and Technology (NIST) Cybersecurity Framework" and gap assessments.).

[18] Transcript from March 28, 2019 Technical Conference at 78:18-19 (Atkins, AEP CEO), *Security Investments for Energy Infrastructure Tech. Conferences*, Docket No. AD19-12-000 (Apr. 26, 2019), eLibrary No. 20190426-4001 (stating that investments in resiliency and reliability of the grid are "really probably one of [the] least risky investments we can make.") ("Security Conference Transcript").

[19] Written Statement of Kevin G. Wailes of Lincoln Electric System 7, *Security Investments for Energy Infrastructure Tech. Conference*, Docket No. AD19-12-000 (Apr. 2, 2019), eLibrary No. 20190402-4009; *see also* Security Conference Transcript at 66:18-24 (Akins) (explaining that "it goes to operational excellence and if your brand is built around operational excellence and you see it as a really something that can really diminish the brand, there's nothing worse that could happen to a company in our opinion to have a significant outage caused by any event, but let alone a cyber event.").

[20] NIST U.S. Resilience Project at 4.

[21] Security Conference Transcript at 151:5-7.

[22] Notice of White Paper 9 n.26-28, *Cybersecurity Incentives Policy White Paper*, Docket No. AD20-19, (June 18, 2020), eLibrary No. 20200618-4003 (citing *Extraordinary Expenditures Necessary to Safeguard Nat'l Energy Supplies*, 96 FERC ¶ 61,299, at 62,129 (2001), *Boston Edison*, 109 FERC ¶ 61,300, P 40 (2004), *Policy Statement on Matters Related to Bulk Power Sys. Reliability*, 107 FERC ¶ 61,052 (2004)) ("Staff White Paper").

themselves,[23] led then-Commissioner Glick to conclude "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."[24]

2. The proposed incentives will impose significant, unnecessary costs on ratepayers.

As then-Chairman Danly and then-Commissioner Glick said in their concurring statement, the question at "the heart of what the NOPR intends to achieve" is "whether public utilities are not adopting the contemplated measures because the existing financial incentives are insufficient."[25] As discussed above, the existing financial incentives are already sufficient to induce utilities to make prudent, above-and-beyond cybersecurity investments. Thus the NOPR's proposed financial incentives would increase consumer costs without providing any incremental consumer benefit. In fact, the NOPR's proposal could reduce security if a utility's existing, security-enhancing investment plans are jettisoned to seek the CIP Incentive (which, as discussed below, will not always improve security).

The NOPR's proposal is legally deficient because it does not demonstrate that its proposed financial incentives are needed to induce the desired level of cybersecurity investment.[26] As noted, the NOPR lacks evidence that *any* financial incentives are

---

[23] *See, e.g.* Exelon Post Technical Conference Comments 1, *Security Investments for Energy Infrastructure Technical Conference*, Docket No. AD19-12-000 (May 28, 2019), eLibrary No. 20190528-5161 ("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.").

[24] Security Conference Transcript at 187:22-24.

[25] NOPR P 3 (Danly, Comm'r, Glick, Comm'r, concurring).

[26] *See* Section II.A, above.

needed. And even if some incentive could be justified, the NOPR's proposed incentives have not.

First, the NOPR provides no justification for setting the ROE Incentive at 200 basis points, which is higher than the vast majority of ROE incentives that the Commission has granted in the past decade.[27] The Commission has an obligation to determine the minimum ROE that will induce the desired investment,[28] yet the NOPR contains no analysis of whether 25 basis points or 50 basis points would be sufficient to induce the desired investment.

Second, the NOPR does not explain why a utility would prefer to "defer and amortize eligible costs"[29] over five years instead of recovering those costs immediately. If a utility's authorized rate of return closely approximates the utility's weighted average cost of capital, then the utility should be indifferent to immediate cost recovery or deferred recovery at the authorized rate of return.

Third, the NOPR's open-ended invitation for public utilities to request "other types of incentives"[30] beyond the proposed ROE and deferred cost recovery incentives reflects an admission that the NOPR has not fully analyzed whether the proposed incentives will produce the desired level of investment in prudent cybersecurity measures. An undefined incentive, to be considered on a case-by-case basis in future

---

[27] The exceptions prove the rule. *See Atl. Grid Operations A LLC*, 135 FERC ¶ 61,144, PP 7, 128 (2011) (reducing a requested 300 basis point ROE incentive to 250 basis points); *Primary Power, LLC*, 131 FERC ¶ 61,015, PP 8, 152 (2010) (reducing a requested 300 basis point ROE incentive to 200 basis points), *order on reh'g*, 140 FERC ¶ 61,052 (2012), *pet. for review dismissed sub. nom, Pub. Serv. Elec. & Gas Co. v. FERC*, 783 F.3d 1270 (2015).

[28] *City of Detroit*, 230 F.2d at 817; *see also supra* note 10.

[29] NOPR P 42.

[30] *Id*. P 47.

proceedings, cannot satisfy the FPA's requirement that just and reasonable incentives be "in fact needed, and no more than is needed, for the purpose."[31]

The NOPR states that "the dollar amounts provided under the incentives should not have a burdensome effect on the public utility's rates."[32] But that statement is both unsupported and incorrect. As reflected in the Commission's order approving Duke Energy's request for special accounting treatment for its Cybersecurity Informational Technology-Operational Technology Program, Duke Energy has "ma[d]e over $137 million in capital investments as part of its Cybersecurity Program" that is "designed based on the [NIST Framework]."[33] That large sum illustrates that cybersecurity investments are not, as the NOPR claims, "relatively small . . . compared to conventional transmission projects."[34] Cybersecurity investments being made outside the electricity industry (without any guaranteed cost recovery, much less financial incentives) confirm the potential magnitude: JP Morgan plans to invest $600 million annually;[35] Microsoft, $1 billion;[36] and the Department of Defense, $9.8 billion.[37]

TAPS recognizes that the NOPR proposes that: ROE incentives would be capped at the top of the zone of reasonableness; both the ROE Incentive and Regulatory Asset

---

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

[32] NOPR P 38.

[33] *Duke Energy Corp.*, 169 FERC ¶ 61,232, P 6 (2019).

[34] NOPR P 38.

[35] Jamie Dimon, Chairman and CEO, *Letter to Shareholders*, JP Morgan 35 (Apr. 3, 2019), https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/ceo-letter-to-shareholders-2018.pdf.

[36] Tova Cohen, *Microsoft to Continue to Invest Over $1 Billion a Year on Cyber Security*, Reuters (Jan. 26, 2017), https://www reuters.com/article/us-tech-cyber-microsoft-idUSKBN15A1GA.

[37] U.S. Dep't of Defense, *DOD Releases Fiscal Year 2021 Budget Proposal*, (Feb. 10, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/.

Incentive would be limited in duration; and utilities would not be permitted to receive both the ROE Incentive and Regulatory Asset Incentive for the same investment.[38] While certainly necessary should the Commission proceed with the NOPR's proposal, these limitations are not sufficient to make the proposed incentives just and reasonable.

In short, ratepayers are already funding substantial investments in utility cybersecurity that go above and beyond mandatory requirements; adding large financial incentives on top will place a heavy burden on ratepayers without commensurate benefit.

3. The Commission should consider low-cost, high-impact incentives, such as public recognition of cybersecurity excellence.

Given the absence of need for and cost burden created by the proposed incentives, FERC should consider other effective, less costly options to incent utilities to go-above-and beyond in cybersecurity. For example, the Commission could publicly recognize industry excellence in cybersecurity.[39] In addition to its low cost, public recognition offers many benefits. It provides positive examples for other utilities to model, promotes industry best practices, and doing so in cybersecurity expands the scope of efforts to recognize utilities that excel in reliability in general.[40] Such endorsements can stimulate competition among utilities to improve their cybersecurity posture.

---

[38] NOPR PP 38, 58.

[39] It is the corollary to the negative reinforcement of publicly disclosing those that fail to meet mandatory NERC CIP Standards.

[40] *See e.g*, Smart Energy International, *FPL receives national award for excellence in reliability* (Nov. 23, 2016), https://www.smart-energy.com/regional-news/north-america/fpl-award-excellence-reliability/ (Florida Power and Light proudly announced that it was the recipient of the ReliabilityOne National Reliability Excellence Award for a second year in a row.); Paul Ciampoli, *Public power utilities earn top customer satisfactions scores*, American Public Power Association (July 15, 2019), https://www.publicpower.org/periodical/article/public-power-utilities-earn-top-customer-satisfaction-scores (refererencing utilities earning top rankings in J.D. Power's customer satisfaction study, driven in part by "focusing their efforts on improving reliability"); U.S. News & World Report, *Energy Rankings - Measuring States' Energy Infrastructure*, Best States Ranking, https://www.usnews.com/news/best-

Today, utilities that are recognized for their cybersecurity efforts (albeit not by the Commission) feature cybersecurity strength as part of their brand, and proudly share those honors in their investor-relations publications.[41] This Commission's *imprimatur* would have an even greater impact.

C. The NERC CIP Incentives Approach should not receive a rebuttable presumption of materially enhancing BES cybersecurity.

The NOPR proposes two types of investments that would qualify for an incentive under the NERC CIP Incentives Approach: the Med/High Incentive and the Hub-Spoke Incentive.[42] As discussed below, neither approach is likely to materially enhance security in all circumstances—and in some cases may be counterproductive. Thus, these proposals contradict the FPA's requirement that the Commission identify the consumer benefits that will result from an incentive.[43] The Commission should therefore not apply a rebuttable presumption that the NERC CIP Incentives Approach will benefit consumers. Instead, a public utility should have the burden of demonstrating that applying the standards to the particular facilities considered will have a material benefit to security that significantly outweighs the costs, including the proposed incentives.

---

states/rankings/infrastructure/energy (last visited Mar. 29, 2021) (Grid reliability was one of three categories specifically ranked).

[41] NIST U.S. Resilience Project at 10. ("In recognition of Exelon's innovative programs and leadership efforts, the Corporate and Information Security Services organization was honored by Security Magazine as the top security organization in the power, electric, gas, nuclear and hydro utilities sector in 2012, 2013, 2014") (citing Exelon, *Exelon Corporation Sustainability Report*, http://www.exeloncorp.com/assets/newsroom/docs/csr/pdf/EXL_SR_2013_pg87-92.pdf) (last visited March 23, 2021)).

[42] NOPR P 25.

[43] *Pub. Utils. Comm'n of Cal. v. FERC*, 367 F.3d at 929; s*ee* Section II.A above.

1. The Med/High Incentive would induce public utilities to make costly investments that do not necessarily enhance security and may well be counterproductive.

Compared to medium and high impact BES Cyber Systems, low impact BES Cyber Systems encompass a much greater diversity of asset types. While CIP-002-5.1a enumerates a list of assets associated with medium and high impact BES Cyber Systems, the low impact category is a catchall, including all BES Cyber Systems not classified as medium or high impact.[44] Given the wide diversity of systems and configurations of low impact BES Cyber Systems, NERC and the Commission have rightly allowed registered entities flexibility in how to achieve security goals for their low impact BES Cyber Systems. For example, when NERC first proposed expanding CIP standards to include low impact BES Cyber Systems (which until then had not been subject to any standards), it explained that an "overriding concern was that by mandating specific controls, the Reliability Standards would ultimately stunt the development of the range of controls necessary to protect the diversity of Low Impact assets now subject to the CIP Reliability Standards."[45]

More recently, in response to a Commission's directive related to electronic access controls for low impact BES Cyber Systems, NERC proposed modifications in CIP-003-7 that established a security objective and provided ten different conceptual frameworks for achieving that objective, recognizing that "there are many different technical solutions that can be used to implement electronic access controls" for low

---

[44] NERC, *CIP-002-5.1a – Cyber Security – BES Cyber System Categorization*, Attach. 1, https://www nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf (last visited Mar. 29, 2021).

[45] Comments of NERC on the Notice of Proposed Rulemaking for Version 5 Critical Infrastructure Protection Reliability Standards 21, *Version 5 Critical Infrastructure Protection Reliability Standards*, Docket No. RM13-5-000 (June 24, 2013), eLibrary No. 20130624-5173.

impact BES Cyber Systems.[46] The Commission initially proposed to direct NERC to further modify the standard to "provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems," due to concerns that auditors would not be able to assess whether the solutions implemented by a utility were reasonable.[47] The Commission suggested that the standards for medium and high impact BES Cyber Systems could serve as "a possible model" for the low impact standard.[48] In the final rule, however, the Commission declined to adopt the proposed directive, because it was "persuaded by commenters" that NERC's original proposal "provide[d] a clear security objective."[49] One of those persuasive commenters was NERC itself, which explained that the proposed standard (which was ultimately accepted) offered more flexibility in implementation for low impact BES Cyber Systems rather than the "prescriptive" approach used for medium and high impact BES Cyber Systems "due to the wide array of low impact BES Cyber Systems and their lower risk to bulk electric system reliability."[50]

A closer examination of a few standards demonstrates that not all the CIP Standards designed for medium impact BES Cyber Systems will be appropriate to apply to low impact BES Cyber Systems. For example, CIP-006-6, Requirement R1.10 requires restriction of physical access to cabling and other nonprogrammable communication components used for connection between assets in a single electronic

---

[46] Petition of NERC for Approval of Proposed Reliability Standard CIP-003-7, at 25, *N. Am. Elec. Reliability Corp.*, Docket No. RM17-11 (Mar. 3, 2017), eLibrary No. 20170303-5213.

[47] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 161 FERC ¶ 61,047, P 3 (2017).

[48] *Id.* P 31.

[49] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 163 FERC ¶ 61,032, P 27 (2018).

[50] *Id.* P 22.

security perimeter.[51] While that may be feasible and appropriate for an 1800 MW generating facility, applying that same requirement to low impact BES Cyber Systems may be neither feasible nor sensible. For example, application to a low impact generating facility with a distributed control system could harm reliability, because many such low impact generating facilities have distributed control systems contained in separate buildings spread across a plant site. As a result, applying CIP-006-6 to such facilities could require installation of firewalls in spaces that were never designed for that kind of setup.[52] This would not only be excessively costly, but it could be counterproductive to security objectives, adding unnecessary complexity (with added points of potential failure) to an otherwise low risk facility.

In short, the NOPR's proposal calls for an across-the-board application of standards designed for one category of assets to another category of assets for which those standards may or may not be appropriate.[53] The Commission therefore cannot presume the proposed Med/High Incentive will materially enhance security.

2. The Hub-Spoke Incentive will be difficult to implement and could induce public utilities to make counterproductive system reconfigurations.

The NOPR proposes to grant an incentive, and a presumption of consumer benefits, to utilities that implement the Hub-Spoke Incentive: ensuring that all cyber

---

[51] NERC, *CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems*, https://www nerc.com/pa/Stand/Reliability%20Standards/CIP-006-6.pdf (last visited Mar. 29, 2021).

[52] If it is infeasible to restrict physical access to cabling between buildings on a plant site, each building with a low impact BES Cyber System would require its own Electronic Security Perimeter, in which case CIP-005-6 would require a firewall (or other Electronic Access Point) for communications between the Electronic Security Perimeters.

[53] Moreover, the NOPR proposes to apply the CIP Standards to non-BES assets, such as corporate IT systems. NOPR P 35. As discussed in Section II.E.2 below, that proposal would not be cost effective nor necessarily security enhancing.

communications to and from a low impact BES Cyber System must connect through a medium or high impact BES Cyber System. Because this proposal is ambiguous as to how it will be implemented, and may not result in benefits to consumers, it does not satisfy the requirements for just and reasonable incentives.[54]

Implementing the NOPR's Hub-Spoke Incentive proposal entails significant ambiguities. Consider, for example, a low impact BES Cyber System that has a single external connection to its Balancing Authority's medium-impact automatic generation controller. In that simple example, the Hub-Spoke Incentive will have been satisfied. But what if the low-impact system has a second external connection to its Reliability Coordinator's high-impact system? Would that render the low-impact system into a "hub" rather than a "spoke" in the NOPR's framework?

Similarly, the NOPR does not explain how a public utility with *only* low impact BES Cyber Systems could implement the Hub-Spoke Incentive. Would such a utility have to route all of its low impact system communications through a third-party's medium impact system? The NOPR does not address the obligations of such a third-party in such a configuration, nor whether such a configuration would enhance security.

These are just two examples of the many different configurations that could result from the Hub-Spoke Incentive. Some of those configurations may well enhance security, but others remain too undefined to assess (and yet others, as discussed below, could harm security). Because the NOPR has not adequately explored the potential configurations, granting a rebuttable presumption of enhanced security would be inappropriate.

---

[54] *See* Section II.B, above.

More fundamentally, TAPS is concerned that the proposed Hub and Spoke Incentive could be counterproductive to reliability and security. TAPS questions whether reconfiguring systems so that all low impact communication flow through a single point would be consistent with other mandatory NERC Standards. NERC Standard TOP-001-4 requires TOs to "have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center."[55] The Hub-Spoke Incentive could encourage utilities to *reduce* the diversity of data exchange infrastructure, thus decreasing reliability and increasing security risk. Thus, the proposed incentive could undermine the important objective of other mandatory standards.

D. The NIST Framework Approach is not clear on the scope of activities that will qualify for an incentive, and the examples provided will not always produce consumer benefits.

The Incentive Policy Statement requires that Section 205 incentives "be understood by all parties."[56] The NOPR's proposed NIST Framework Approach is too ambiguous to comply with that requirement, because it does not adequately define what types of investments would qualify for the incentive.

The proposed NIST Framework Approach would grant incentives for "implementing certain security controls included in the NIST Framework" and proposes "to initially only consider incentives that fall within the . . . automated and continuous monitoring" type of security controls.[57] The NIST Framework does not, however,

---

[55] NERC, *TOP-001-4 – Transmission Operations*, R 20, https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-4.pdf (last visited Mar. 29, 2021).

[56] Incentive Policy Statement at 61,590.

[57] NOPR PP 32-33.

identify a category of controls related to *automated* monitoring. In fact, the term "automated and continuous monitoring" does not appear anywhere in the NIST Framework. The NIST Framework's Continuous Monitoring (DE.CM) category contains a host of subcategories, that include monitoring of physical environments, personnel activity, and external service providers—none of which are "automated." The NOPR provides no indication of whether some, all, or none of the security controls described in those subcategories will be eligible for an incentive.[58] The NOPR provides three examples of the kind of security controls that might qualify,[59] but those examples do not limit or define the full scope of activities that would be eligible for incentives.

The NOPR's examples of potentially qualifying investments pose a separate impediment to ensuring the proposed incentives are just and reasonable: the benefits of those investments cannot be easily assessed or understood.[60] Consider the NOPR's example of a dynamic asset management program that would allow a utility to "quickly detect and address new or previously unknown equipment."[61] Such a program would not be a prudent investment for a small, relatively static, system, on which non-automated approaches would be equally effective at identifying new or unknown equipment. Even for a larger system that changes more frequently, a dynamic asset management system would be effective only if the utility has reached a sufficient level of cybersecurity maturity.

---

[58] The NOPR cites to the Staff White Paper at 19, but that document sheds little additional light on the scope of security controls that would be included in the incentive proposal.

[59] NOPR PP 33-35 (describing "tools that utilize automated features for pulling information from a variety of sources," "install[ing] a dynamic asset management program," and "implementation of a dynamic file analysis program.").

[60] *See* Section II.C above.

[61] NOPR P 34.

Ultimately, the proposed NIST Framework Approach is a "flexib[le]" and "non-prescriptive" option.[62] That flexibility may well be appropriate, given the diverse systems around the country.[63] But that flexibility renders the proposal overly vague for the purpose of granting incentives. That is especially true given the lack of opportunity for meaningful customer comments in the proposed application process.[64]

E. The proposal's scope should be clarified and narrowed.

The NOPR proposes granting incentives pursuant to Section 205, rather than Section 219, because Section 219 is limited to transmission while Section 205 gives the Commission authority "to provide incentives for cybersecurity investment not only in transmission facilities but also for cybersecurity investment in information technology and operational technology networks that a public utility uses to provide other jurisdictional services."[65] Those "other jurisdictional services" include the sale of electric energy at wholesale, as well as investments made to a utility's general plant facilities.[66] The Commission should clarify how, if at all, the incentives would apply to non-transmission facilities; and it should narrow the scope of those incentives. Otherwise, the proposal would violate the principle that Section 205 incentives "be understood by all parties."[67]

---

[62] *Id.* P 32.

[63] And, as discussed in Section II.B above, utilities are already using such flexible approaches under the Commission's existing cost recovery mechanisms.

[64] *See* Section G, below.

[65] NOPR P 20 (footnote omitted).

[66] *See*, *id.* P 39 (discussing incentives for general plant facilities).

[67] Incentive Policy Statement at 61,590; *see* Section II.A above.

1. The Commission should not grant incentives to generators with market-based rates.

The NOPR does not explain how either the ROE Adder Incentive or Regulatory Asset Incentive would apply to generators with market-based rate authority, which make up the majority of generation under the Commission's jurisdiction. Because such generators do not earn a regulated ROE, neither of the NOPR's proposed incentive mechanisms would be applicable. If, however, a final rule were to include an open-ended invitation for alternative forms of incentives (as the NOPR contemplates)[68] generators may well request such incentives. Any financial incentive for a generator with market-based rates will have the potential to distort the competitive energy and ancillary services markets that the Commission relies on to ensure just and reasonable rates for wholesale power.

2. The Commission should not grant incentives for non-BES assets, such as corporate IT systems.

The NOPR contemplates granting incentives for cybersecurity investment made to a utility's general plant facilities, including its corporate IT systems.[69] Citing the WANNACRY attack, the NOPR explains that, while corporate IT servers are less critical to reliable operations, securing those systems could nevertheless improve reliability of the Bulk-Power System.[70] But the NOPR glosses over how its specific incentive proposals—the NERC CIP Approach and the NIST Framework Approach—would be applied to corporate IT systems.

---

[68] NOPR P 47.

[69] *Id.* P 39.

[70] *Id.*

As an initial matter, as discussed in Section II.A above, there is no evidence that utilities require additional financial incentives to implement prudent security measures on their corporate IT systems. Moreover, for many public utilities, the "conventionally allocated portion of such investments that flows through to Commission jurisdictional cost-of-service rates" is small.[71] Most of the rate recovery for general plant is subject to state regulatory jurisdiction. Cybersecurity measures for a corporate IT system must be applied to the entire system to be effective, so a public utility's decision to invest in such measures will be driven by state—not federal—policy. The NOPR's proposed incentives will burden transmission customers with higher rates with little chance of inducing the investment intended to be incented.

Furthermore, applying the NERC CIP Approach to general plant facilities, such as corporate IT systems, could result in illogical results. As discussed in Section II.C above, across-the-board application of CIP Standards designed for medium and high impact systems could be counterproductive for low impact systems; that problem is magnified when considering how to apply CIP Standards to corporate IT systems. Similarly,

---

[71] *Id.*; *see e.g.*, Annual Formula Transmission Rate Update Filing for Rate Year 2021 of Pacific Gas and Electric Company, Attach. B, Tab 24 line 113, Docket No. ER19-13-000, et al. (Dec. 1, 2020), eLibrary No. 20201201-5280 (allocating 7.2% of general plant to transmission function); Atlantic City Electric Company, Informational Filing of 2020 Formula Rate Annual Update; Notice of Annual Update, Attach. H-1A, Allocators, line 5, Docket No. ER09-1156 (May 15, 2020), eLibrary No. 20200515-5176 (Wages & Salary Allocator of 10.72%); Entergy Arkansas, LLC Annual Informational Attachment O Filing, Formula Rate –Appendix A, Line 11, Docket No. ER21-1429-000 (Mar. 15, 2021), eLibrary No. 20200315-5351 (Transmission Wages and Salaries Allocation Factor 5.8%); Niagara Mohawk Power Corporation d/b/a National Grid, Informational Filing of Niagara Mohawk Power Corporation of the Annual Update to the Formula Transmission Service Charge Under the NYISO Open Access Transmission Tariff, Attach. 1 to Attach. H, Schedule 5, line 3, Docket No. ER08-552-000 (June 15, 2020), eLibrary No. 20200615-5128 (Allocation Factors, Line3) (Transmission Wages and Salaries Allocation Factor of 13.0%); Annual Informational Filing of NSTAR Electric Company 7, Docket No. ER07-549-000- (June 1, 2020), eLibrary No. 20200601-5152 (Sheet 3, Line 2 showing Transmission Wages and Salaries Allocation Factor of 12.9%).

applying the Hub-Spoke Approach would not be feasible for general plant facilities; a utility could not reasonably ensure all communications from a utility's corporate IT system—its web pages, email, customer communications, etc.— are routed through a medium-impact BES Cyber System. Yet that is precisely what the NOPR's proposal would incentivize.

F. The proposals weak verification mechanisms and the lack of any meaningful consequences for non-compliance render the proposal unjust and unreasonable.

The NOPR proposes to grant incentives without any mandatory audits or duty to self-report non-compliance, and imposes no penalty for non-compliance. That renders the incentive proposal unjust and unreasonable.

Especially for the Med/High Incentive, the lack of compliance monitoring comparable to that of NERC's compliance monitoring will prevent the Commission—and ratepayers—from knowing whether a public utility has indeed provided the incentivized security benefits. Annual self-certification, as proposed by the NOPR, is inadequate. NERC has both a self-certification requirement and a self-report program, yet more than one in five incidents of non-compliance are identified through audits or investigations.[72] By excluding any formal audit program, the NOPR's proposal will leave a significant percentage of non-compliance undetected.

The lack of serious compliance monitoring is compounded by the proposal's lack of any penalty for non-compliance. The Incentive Policy Statement requires that Section 205 incentives be symmetrical: "opportunities for reward should be offset by a symmetric

---

[72] NERC, *Compliance Monitoring and Enforcement Program Annual Report*, Appendix A at 28 (Feb. 5, 2020), https://www nerc.com/pa/comp/CE/ReportsDL/2019%20Annual%20CMEP%20Report.pdf.

downside risk."[73] The NOPR proposes no such symmetry. The only penalty for non-compliance is losing the incentive during the period of non-compliance. Under that circumstance, a public utility has a financial incentive to hide non-compliance. Certainly, a utility would have no financial incentive to invest in the internal controls and monitoring that would allow the utility to even be aware of non-compliance.

Furthermore, the lack of a self-reporting mechanism for the NERC CIP Incentives approach could undermine a utility's efforts to analyze its security posture in a holistic manner. Utility employees are trained to identify and promptly self-report potential incidents of non-compliance with the medium and high impact NERC CIP Standards, if they are being mandatorily applied to medium and high impact BES Cyber Systems. Those same employees will now be trained *not* to self-report non-compliance with the same NERC CIP Standards, if the standards are being voluntarily applied to low or medium impact BES Cyber Systems. The NOPR's proposal could incentivize a public utility to keep "two sets of books" for compliance violations—one to self-report to NERC and the other for voluntary compliance infractions. Such an approach is "inconsistent with ongoing efforts to improve the culture of compliance in registered entities."[74]

G. Customers must have a meaningful opportunity to evaluate and comment on any incentive requests.

The Commission's Incentive Policy Statement explained that Section 205's just and reasonable standard requires that incentive applicants to "be specific and clearly state the expected benefits relative to cost-of-service regulation" and that the "incentive

---

[73] Incentive Policy Statement at 61,590.

[74] *N. Am. Elec. Reliability Corp.*, 138 FERC ¶ 61,193, P 58, *on reh'g*, 139 FERC ¶ 61,168 (2012); *see also Revised Policy Statement on Enforcement*, 123 FERC ¶ 61,156, P 57 (2008) (placing importance on a "culture that encourages compliance among company personnel."); *Policy Statement on Compliance*, 125 FERC ¶ 61,058 (2008).

mechanism[] . . . be understood by all parties."[75] The NOPR's procedures for review of incentive applications do not satisfy that standard because the procedures do not afford customers adequate time or information to understand the specific benefits of a public utility's incentive proposal.

The NOPR proposes to allow applicants to redact Critical Electric Infrastructure Information ("CEII") related to its cybersecurity systems, consistent with the Commission's filing regulations.[76] The NOPR "expects" such redactions to be "specific and limited" and that the public portion of the application will "contain sufficient information for ratepayers to judge the rate impact and scope of the proposed incentives."[77] But the NOPR does not state an expectation that applicants should publicly make available information pertinent to the crucial question of whether the investment will materially enhance security. That omission is made all the more concerning by the NOPR's recognition that meaningfully evaluating an application's potential security benefits involves a fact-specific inquiry into the "utility's existing attributes," its "system configuration," the "specific characteristics" of the investment, and more.[78] Much, if not all, of that information that the NOPR deems necessary is likely to be redacted as CEII. In fact, a filing utility has incentive to overuse CEII designations—both to protect its security and to avoid ratepayer scrutiny—while the Commission's regulations provide no mechanism to discipline such overuse.

---

[75] Incentive Policy Statement at 61,600.

[76] NOPR P 74 (citing 18 C.F.R. § 388.113).

[77] *Id.* P 75.

[78] *Id.* P 55.

The Commission's usual filing procedures under Section 205 provide only twenty-one days for a customer to: discover that an application has been made; submit an intervention and execute a protective agreement;[79] wait up to five business days for the applicant to provide the unredacted application;[80] analyze the complex, technical data; and prepare a protest or comments to submit to the Commission. And the Commission is required to issue an order within sixty days. Such a compressed timeline will prevent an incentive application from receiving the kind of meaningful Commission and customer evaluation necessary to ensure just and reasonable rates. To avoid arbitrary decisions that lack substantial evidence, the Commission should make clear that all cybersecurity incentive applications will be presumed to raise issues of material fact, and will thus be subject to an evidentiary hearing with opportunity for discovery.[81] Such a presumption will ensure that the Commission's CEII regulations are properly used to limit dissemination of any CEII without allowing those same regulations to be used as a shield for utilities to avoid scrutiny of their rates.

H. The Commission should not mandate the best practices contemplated in this NOPR.

In their concurring statement, then-Chairman Danly and then-Commissioner Glick encouraged commenters to address "whether the Commission can 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"

---

[79] 18 C.F.R. § 388.113(g)(4).

[80] *Id.* (if the applicant objects to disclosure, a customer could wait even longer than five business days).

[81] *Idaho Power Co.*, 117 FERC ¶ 63,050, P 12 (2006) ("genuine issue[s] of material fact in dispute . . . must be adjudicated in a trial-type hearing.").

rather than act through incentives.[82] They went on to state that "the importance of cybersecurity demands us to at least consider whether we should mandate the best practices contemplated in this NOPR rather than simply trying to induce public utilities to adopt them."[83] TAPS agrees that cybersecurity is very important. While we oppose the proposed incentives as neither necessary nor effective in advancing cybersecurity, the answer is *not* to "mandate the best practices contemplated in this NOPR."

There are many reasons why the Commission should not consider using its authority to direct development of standards to mandate the practices proposed to be incented in this NOPR. First, as explained in Section II.C above, neither of the practices described in NOPR's NERC CIP Incentives Approach—i.e., the Med/High Incentive and the Hub-Spoke Incentive—will always benefit security and, in some cases, those practices will be counterproductive. For the same reason, mandating those practices—e.g., by directing that all the medium impact standards be made mandatory for a set of low impact BES Cyber Systems—would not be "just, reasonable, not unduly discriminatory or preferential, and in the public interest,"[84] as statutorily required for mandatory standards. Nor would a broad-brush application of prescriptive CIP standards be well designed to address "instability, uncontrolled separation, or cascading failures[,]" as is also required by the Federal Power Act.[85] In a similar vein, mandating the practices

---

[82] NOPR P 2 (Danly, Comm'r, Glick, Comm'r, concurring).

[83] *Id.*

[84] FPA Section 215(d)(2), 16 U.S.C. § 824*o*(d)(2).

[85] *Id.* Section 215 (a)(4), 16 U.S.C. § 824*o*(a)(4). Separately, the Commission has initiated an inquiry into whether the CIP Standards should be modified to address any potential gaps between the existing standards and the NIST Framework. *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, 171 FERC ¶ 61,215 (2020). And NERC is engaged in existing processes to further revise the CIP Standards. *See* NERC, Information Filing Regarding Standards Development Projects, *N. Am. Elec. Reliability Corp.*, Docket RD20-2-000 (Mar. 15, 2021), eLibrary No. 20210315-5427.

discussed in the NOPR's NIST Framework Approach would not be just and reasonable because, as explained in Section II.D, the practices are too ambiguous to lend themselves to enforceable reliability standards.

Second, NERC has additional tools, beyond mandatory standards, that are more effective at addressing evolving cybersecurity threats. The NOPR correctly recognizes that, while mandatory CIP Standards have an important role to play in ensuring cybersecurity, there are limits to how quickly mandatory standards can become effective.[86] But NERC can employ other security-enhancing activities, including: assessments, reports, and studies; alerts and lessons learned issuances; collaboration on risk prioritization with stakeholders; information sharing; and simulated training exercises. NERC has explained to the Commission the massive scope of its "defense-in-depth" efforts to ensure BES cybersecurity.[87] In its comments to the Commission's notice of inquiry in Docket RM20-12-000, NERC described specific security guidelines it has developed,[88] the work of its E-ISAC,[89] its collaboration with industry associations,[90] and its recent alerts.[91] Rather than directing NERC to develop new standards to mandate

---

[86] NOPR P 18.

[87] *See, e.g.*, NERC, Joint Comments in Response to Notice of Inquiry, *Equipment & Servs. Produced or Provided by Certain Entities as Risks to Nat'l Security*, Docket No. RM20-19-000 (Nov. 23, 2020), eLibrary No. 20201123-5101; NERC, Joint Comments in Response to Notice of Inquiry, *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, Docket No. RM20-120-000 (Aug. 24, 2020), eLibrary No. 20200824-5251 ("NERC CIP NOI Comments").

[88] NERC CIP NOI Comments at 13-14. *See also* NERC, *Reliability and Security Guidelines*, https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx (last visited Mar. 29, 2021) (showing 21 approved security guidelines and 3 draft guidelines).

[89] NERC CIP NOI Comments at 14.

[90] *Id.* at 18-19.

[91] *Id.* at 17-18. *See also* NERC, *Alerts*, https://www nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx (last visited Mar. 29, 2021) (showing four alerts in the past year, all aimed at addressing emerging cybersecurity issues).

the practices that the NOPR proposes to incent, the Commission should acknowledge that effective utilization of NERC's non-standard tools can play a powerful role in mitigating evolving cybersecurity threats, and work with NERC to enhance such usage.

Third, mandating the "best practices" proposed to be incented in the NOPR would be fundamentally at odds with the "risk-based approach [to cybersecurity] reflected in the CIP version 5 Standards."[92] The Commission has explained that its directives are intended to be in accordance with that approach, which requires NERC to design standards "to address the risk posed by the assets being protected."[93] That means standards for low impact BES Cyber Systems "may be less stringent" than those for medium or high impact systems, "commensurate with the risk."[94] Thus, a risk-based approach to standards requires such standards to be "appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."[95] Mandating the practices proposed to be incented in the NOPR, so that the standards designed for higher risk BES Cyber Assets would indiscriminately apply to lower impact BES would violate that principle, resulting in compliance burdens that far outweigh the identified risk.

In addition, mitigation measures, especially for low impact BES Cyber Systems, should be flexible and results-oriented. NERC has long stated an intent to move towards results-based standards that identify *what* a utility should achieve instead of *how* a utility should achieve it. The benefit of a results-based standard is that it is inherently adaptable

---

[92] *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).

[93] *Id.*

[94] *Id.*

[95] *Id.* P 53.

to changing circumstances—as long as the desired result remains the same, it doesn't matter if the means to achieve it change over time.[96] Yet many of the CIP standards applicable to medium and high impact BES Cyber Systems are prescriptive and inflexible, and would not be well-suited (or even helpful) for application to low impact BES Cyber Systems that are quite different from the BES Cyber Systems for which the standards were designed.

If the Commission were to nevertheless consider going down such a path, it should adopt an approach that is much more risk-based, cautious, and tailored. For example, there is a significant difference in cyber risk among various low impact BES Cyber Systems. For example, BES Cyber Systems associated with a 25 MW generator and a 1,499 MW generator are both considered low impact, though the reliability risk is obviously greater for the larger generator. To address those realities, it may be appropriate to explore further subdividing the low impact category. However, doing so, consistent with the CIP Reliability Standards' risk-based framework, will not be as simple as changing voltage or MW thresholds for the medium-impact category. A more nuanced approach to subdividing low impact BES Cyber Systems is likely to be more effective. Further study and analysis are needed to determine how best to more granularly delineate risk categories within the low impact category.

---

[96] Implementation Guidance or other tools can be used to establish safe harbors, so that registered entities can be sure that a particular method will be deemed compliant in particular circumstances.

CONCLUSION

The Commission should consider TAPS comments when acting on this NOPR, which TAPS urges the Commission *not* to adopt as a final rule.

Respectfully submitted,

/s/ Cynthia S. Bogorad

Cynthia S. Bogorad
Latif M. Nurani
Anree G. Little*

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

April 6, 2021

* Admitted to the Maryland Bar and not currently admitted to practice in D.C. His work is supervised by principals of the firm pursuant to D.C. App. R. 49(c)(8).