UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Potential Enhancements to the Critical Infrastructure Protection Reliability Standards	Docket No. RM20-12-000

COMMENTS OF THE
TRANSMISSION ACCESS POLICY STUDY GROUP

The Transmission Access Policy Study Group ("TAPS") appreciates the opportunity to respond to the Commission's June 18, 2020 Notice of Inquiry seeking comments on potential enhancements to the currently effective Critical Infrastructure Protection ("CIP") Reliability Standards.[1] TAPS supports the goal of continuing to secure the grid against physical and cyber threats using risk-based approaches. As the Commission considers changes to the CIP Reliability Standards, particularly for low impact Bulk Electric System ("BES") Cyber Systems, TAPS urges the Commission to adhere to the following principles:

- Mitigation measures should be tailored to the risks identified.
- Any new standards for low impact BES Cyber Systems should allow for flexibility to adopt appropriate controls that are needed to meet the identified objectives, recognizing the greater diversity of assets in the low impact category.
- Rather than directing the development of new or modified Reliability Standards, the Commission should defer to NERC's technical expertise in determining how best to address the identified risks.

[1] *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, 171 FERC ¶ 61,215 (2020) ("Notice of Inquiry").

In addition to those principles, TAPS notes that even if new CIP requirements are warranted for *some* types of low impact BES Cyber Systems, it may not be necessary to apply those requirements to *all* types of low impact BES Cyber Systems. Therefore it may be appropriate to explore possibilities for subdividing the low impact category.

I. 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 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 NERC reliability standards.

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

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

II. COMMENTS

A. Mitigation measures should be tailored to the identified risks.

The Notice of Inquiry identifies two risks associated with low impact BES Cyber Systems: (1) that their compromise could be used to gain access to medium and high impact BES Cyber Systems,[3] and (2) that a coordinated attack on multiple low impact BES Cyber Systems could have significant impact on bulk electric system reliability.[4] The Commission should not use either of these theories of risk to justify an across-the-board application of certain medium impact CIP Reliability Standards to low impact BES Cyber Systems. Instead, any new mitigation measures for low impact BES Cyber Systems should be tailored to address those risks that have been identified.

Tailoring mitigation measures to identified risks is inherent to the CIP Reliability Standards' risk-based approach to cybersecurity.[5] The CIP Version 5 Reliability Standards were the first standards to require that all BES Cyber Systems, even the low impact ones, have at least a baseline level of cybersecurity, commensurate with their risk.[6] Low impact BES Cyber

[3] Notice of Inquiry PP 16, 18.

[4] *Id.* PP 23-28.

[5] *See Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160, P 75 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

[6] *Id*.

Systems, which by definition have the lowest impact on bulk electric system reliability, appropriately had lower cost and more flexible requirements.[7] Since then, under the Commission's direction to "address[] a specific matter,"[8] NERC has developed increasing requirements for low impact BES Cyber Systems that are tailored to identified risks.[9]

Before issuing directives to address the risks identified in the Notice of Inquiry, the Commission, NERC, and the industry should seek to better understand the nature of the risks. The Notice of Inquiry does not cite any studies on the risk of using compromised low impact BES Cyber Systems to gain access to other systems,[10] and the studies cited for the risk of coordinated attack do not fully analyze how such an attack could lead to widespread outages.[11]

Once the risks have been more thoroughly analyzed, appropriate mitigation steps can be taken. Those steps should be tailored to the identified risks. Specifically, mitigation measures—be they new Reliability Standards or other measures—should not increase consumer costs or reduce operational flexibility without providing commensurate security benefits.

For example, if the Commission determines that action must be taken to prevent a compromised low impact BES Cyber System from being used "as a launching point" to gain access to medium and high impact BES Cyber Systems,[12] then the most effective solution might be to place stronger controls around those medium and high impact systems so that they don't inherently trust a low impact system that may have been compromised. In contrast, imposing

[7] *Id.*

[8] 16 U.S.C. § 824o(d)(5).

[9] *See, e.g., Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016); *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Order No. 843, 163 FERC ¶ 61,032 (2018).

[10] *See* Notice of Inquiry P 16.

[11] *See, id.* P 23-28.

[12] *Id.* P 18.

greater controls on low impact BES Cyber Systems may create a false sense of security for medium and high impact BES Cyber Systems to further increase their trust levels in low impact systems.

B. Instead of issuing directives for new standards, the Commission should allow NERC's existing processes to work.

To the extent the Commission determines that mitigation measures are needed to address any of the risks identified in the Notice of Inquiry, it should not issue a directive to NERC to develop a new or modified standard. NERC is already taking a wide range of actions to address cybersecurity risks, including the kinds of risks that are identified in the Notice of Inquiry. Issuing a directive to develop a standard could inadvertently divert resources and focus from NERC's existing and forthcoming initiatives aimed at securing the grid.

As the Commission is aware, NERC currently has multiple standard drafting teams working on improvements to the CIP Reliability Standards.[13] That includes Project 2020-03 – Supply Chain Low Impact Revisions that will "modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary."[14]

New and modified standards are only the tip of the iceberg of NERC's cybersecurity efforts. For example, NERC has the ability to issue Alerts, which can be used to address rapidly

[13] *See Reliability Standards Under Development*, NERC (last accessed Aug. 21, 2020), https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx.

[14] *Standard Authorization Request*, NERC, 1-2 (last accessed Aug. 21, 2020), https://www.nerc.com/pa/Stand/202003_Supply_Chain_Low_Impact_Revisions_DL/2020-03_Supply_Chain_LIR_SAR_04032020.pdf.

evolving cyber threats, and identify recommended or essential mitigation actions.[15] As of last year, NERC had issued forty-one cybersecurity Alerts to the industry.[16] There have been two more since, both related to supply chain cybersecurity.[17] In addition, NERC has the ability to issue guidelines and technical bulletins that can assist the industry in protecting against cyber threats. Just this month NERC, along with Commission staff, issued a useful white paper on assessing infrastructure and the deployment of foreign adversary components that could be used to impact the Bulk Power System.[18]

This range of cybersecurity activities demonstrates that new or revised CIP Reliability Standards are not the only, and sometimes not the most effective, tool in NERC's arsenal. Reliability Standards, developed through an ANSI-compliant, Commission-approved process, have many benefits and can ensure a baseline level of defense-in-depth protection against certain types of risks, but the standard development process does not lend itself to addressing rapidly evolving cybersecurity threats.[19] NERC's other tools can be more effective for some of those risks.

[15] *See* Rules of Procedure, NERC § 810 (Jan. 25, 2019), https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20190125.pdf.

[16] Testimony of James B. Robb Before the House Committee on Energy and Commerce, NERC, 7 (July 12, 2019), https://www.nerc.com/news/testimony/Testimony%20and%20Speeches/House%20Energy%20and%20Commerce%20Cyber%20Hearing%20Testimony%207-12-19.pdf.

[17] *Alerts*, NERC (last accessed Aug. 21, 2020), https://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx.

[18] *Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller*, NERC (July 31, 2020), https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf. .

[19] Cybersecurity Incentives Policy White Paper, *Cybersecurity Incentives Policy White Paper*, Docket No. AD20-19-000 (June 18, 2020), eLibrary No. 20200618-4003.

NERC is best placed to determine which tools to use to address cybersecurity risks. The Commission should defer to NERC's expertise rather than issue a directive that pre-determines that a new or modified Reliability Standard is the only way to address an identified risk.

C. Any new or modified CIP Reliability Standards for low impact BES Cyber Systems should allow for flexible and responsive implementation.

The Notice of Inquiry identifies certain NIST Framework sub-categories that may not be explicitly or fully addressed in the CIP Reliability Standards. Some of those potential "gaps" pertain to all categories of BES Cyber Systems, while others pertain to only low impact BES Cyber Systems. To the extent that the Commission determines that any of these potential gaps require new or modified standards, it should also clarify that any standards for low impact BES Cyber Systems will continue to allow for more flexible and responsive implementation than the CIP Reliability Standards applicable to medium and high impact BES Cyber Systems.

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 included as medium or high impact.[20] Given the diversity of systems and configurations of low impact BES Cyber Systems, NERC and the Commission have quite rightly allowed registered entities flexibility in how to achieve security goals for low impact BES Cyber Systems. For example, when NERC first proposed expanding the CIP standards to include low impact BES Cyber Systems, which until then had not been subject to any standards, it explained that the "overriding concern was that by mandating specific controls, the Reliability Standards would ultimately stunt the development of

[20] *CIP-002-5.1a – Cyber Security – BES Cyber System Categorization*, Attach. 1, NERC (Dec. 14, 2016), https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf.

the range of controls necessary to protect the diversity of Low Impact assets now subject to the CIP Reliability Standards."[21]

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 impact BES Cyber Systems.[22] 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.[23] 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.[24]

In the final rule, however, the Commission declined to adopt the proposed directive.[25] In doing so, the Commission implicitly recognized in that order that, while the more prescriptive controls required for medium and high impact BES Cyber Systems may be easier to audit, more flexibility is needed to ensure the security of low impact BES Cyber Systems. Given the greater diversity of the low impact BES Cyber Systems, indiscriminately applying standards designed for medium and high impact BES Cyber Systems may have the opposite of the intended effect,

[21] 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.

[22] 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.

[23] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 161 FERC ¶ 61,047, PP 29-32 (2017).

[24] *Id.* P 31.

[25] Order No. 843, P 3.

"stunt[ing] the development of the range of controls necessary to protect the diversity of Low Impact" BES Cyber Systems.[26]

Thus, if the Commission determines that new or modified standards are needed for low impact BES Cyber Systems, it should not simply extend the applicability of existing standards applicable to medium and high impact BES Cyber Systems, but rather allow for new standards that are risk-based, flexible, and appropriate for low impact BES Cyber Systems.

D. Further subdivision of the low impact category may be appropriate, but further analysis is warranted.

The Notice of Inquiry identifies some potential "gaps" between the NIST Framework and the CIP Reliability Standards applicable to low impact BES Cyber Systems. As discussed above, to the extent these "gaps" pose reliability risks, the Commission should allow NERC to develop tailored mitigation measures that allow for flexible implementation, which is the best way to address cybersecurity risk for low impact BES Cyber Systems. However, to the extent that the Commission determines that more prescriptive and costly CIP Reliability Standards are necessary for *some* types of low impact systems, it may not be necessary or appropriate to apply those requirements to *all* types of low impact systems.

There is a significant difference in cyber risk between 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.

[26] *See supra*, note 21.

Further subdivision, 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 further delineate risk categories within the low impact category.

CONCLUSION

TAPS urges the Commission to adhere to the principles discussed in these comments as it considers whether further changes are needed to the CIP Reliability Standards.

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

August 24, 2019