UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems	Docket No. RM22-3-000

COMMENTS OF THE
TRANSMISSION ACCESS POLICY STUDY GROUP

The Transmission Access Policy Study Group ("TAPS") appreciates the opportunity to comment on the Commission's January 20, 2022 Notice of Proposed Rulemaking ("NOPR")[1] proposing to direct NERC to develop new or modified reliability standards that will require owners and operators of high and medium impact Bulk Electric System Cyber Systems to implement internal network security monitoring ("INSM") within trusted Critical Infrastructure Protection networked environments.

TAPS urges the Commission to adopt a risk-based approach in any directive issued in this proceeding. In particular, TAPS urges the Commission *not* to direct NERC to require implementation of INSM on low impact Bulk Electric System ("BES") Cyber Systems, because compared to a directive for high and medium impact BES Cyber Systems, the potential reliability benefit is lower while the technical barriers and associated costs are higher. These comments focus on the NOPR's questions related to low impact BES Cyber Systems.

---

[1] *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys.*, 178 FERC ¶ 61,038 (2022).

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.

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

[2] Jane Cirrincione, Northern California Power Agency, is TAPS Chair. Dave Osburn, Oklahoma Municipal Power Authority, is Vice Chair. Terry Huval is TAPS Executive Director.

II. COMMENTS

The NOPR seeks comment on the usefulness and practicality of implementing INSM in networks with low impact BES Cyber Systems. Specifically, it asks about the potential benefits, technical barriers, and associated costs of such implementation. And it asks whether there is an identifiable subset of low impact BES Cyber Systems to which INSM requirements should apply. As discussed in more detail below, TAPS urges the Commission not to expand the NOPR's proposed directive to include low impact BES Cyber Systems, because such expansion will result in:

- **Limited Incremental Reliability Benefit:** Requiring INSM for low impact BES Cyber Systems will provide less benefit than for high and medium impact BES Cyber Systems, because the NOPR's identified threats—escalating privileges, moving laterally within a trust zone, executing unauthorized code—pose a lower risk to BES reliability within low impact BES Cyber systems.

- **Greater Technical Barriers:** Low impact BES Cyber Systems are more diverse than the other impact categories, which will require more customized implementations of INSM packages and thus more highly specialized staff.

- **Significantly Higher Cost:** INSM implementation costs grow substantially as the number of networked devices increase. As a result, in addition to the high cost of overcoming technical barriers of implementing INSM for low impact BES Cyber System, the sheer number of low impact BES Cyber Systems will impose a significant cost burden.

Rather than sweep low-impact BES Cyber Systems into new or modified standards, NERC can more effectively support the security and reliability of the grid by focusing its efforts on its other tools—such as alerts, guidelines, and technical bulletins—

that can help protect low impact BES Cyber Systems against the identified risks in a more flexible and efficient manner.

If the Commission nevertheless directs NERC to develop a new or modified standard to require INSM for a subset of low impact BES Cyber Systems, the Commission should defer to NERC's technical expertise in identifying that subset and provide adequate time for NERC to study an appropriate, risk-based subdivision of the low impact category for the purpose of INSM.

A. Requiring INSM for low impact BES Cyber Systems will impose undue costs on ratepayers without offsetting reliability benefits.

The Commission should not expand the NOPR's proposed directive to include low impact BES Cyber Systems, because the potential reliability benefit is lower while the technical barriers and associated costs are higher.

1. The NOPR's identified threats pose a lower risk to BES reliability within low impact BES Cyber Systems.

The NOPR identifies three threats that can be addressed with INSM—(1) escalating privileges, (2) moving inside the trust zone, and (3) executing unauthorized code—and asks about the risk posed by those threats when applied to networks containing low impact BES Cyber Systems.[3] By definition, the risk associated with low impact BES Cyber Systems is lower than it is for high and medium impact BES Cyber Systems. Federal Power Act Section 215 defines "reliable operation" as operating a system "so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of . . . a cybersecurity incident."[4] Low impact BES Cyber

---

[3] NOPR P 33.

[4] 16 U.S.C. 824o(a)(4).

Systems perform or support BES reliability functions for Facilities that, if rendered unavailable, are less likely to result in such instability, uncontrolled separation, or cascading failure.[5] The risk to BES reliability from a low impact BES Cyber System that controls a single generator pales in comparison to the risk associated with the high impact BES Cyber System in the control center for an entire balancing authority.

2. Implementing INSM for low impact BES Cyber Systems poses greater technical barriers that are impractical to overcome.

Compared to high and medium impact BES Cyber Systems, implementing INSM is more challenging for low impact BES Cyber Systems because of their greater diversity and distinct requirements for electronic access controls.

First, low impact BES Cyber Systems perform or support BES reliability functions for a greater range of Facility 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.[6] The diversity of Facilities associated with low impact BES Cyber Systems results in greater diversity of systems and configurations.

In the experience of TAPS members, available INSM products are not easily configurable for such a wide range of operational technology ("OT") systems. More than a third of locations with only low impact BES Cyber Systems have no external routable connectivity,[7] which makes the monitoring and logging of INSM data very difficult

---

[5] *See 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.

[6] *Id.*

[7] NERC, *Supply Chain Risk Assessment, Analysis of Data Collected under the NERC Rules of Procedure*

unless additional connectivity is added (which would counterproductively increase the security risk). Additionally, low impact BES Cyber Systems use a greater variety of OT communication protocols—e.g., ICCP, Modbus, DNP3—that are not recognized by most INSM products. While specialized products are available for OT communication protocols, configuring those products on the full range of low impact BES Cyber Systems, including systems that include legacy cyber assets, is challenging, especially because implementing such solutions requires coordination with original equipment manufacturers.

The complexity of separately configuring INSM for each unique low impact BES Cyber Systems, and then maintaining and monitoring those systems, makes it impractical. Doing so requires highly skilled staff who are familiar not only with INSM technology but also a wide range of OT environments. Such staff are scarce, so small systems can have difficulty recruiting and retaining individuals with that specialized skillset.

Second, low impact BES Cyber Systems have distinct requirements for electronic access controls, rather than an electronic security perimeter. As the NOPR correctly identifies, INSM requires establishment of a "trust zone" such as an electronic security perimeter.[8] While high and medium impact BES Cyber Systems are required to establish electronic security perimeters,[9] the Commission rightly declined to require low impact

---

Section 1600 Data Request 8 (Dec. 9, 2019), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf ("Supply Chain Risk Assessment").

[8] NOPR P 1.

[9] NERC, *CIP-005-6 — Cyber Security – Electronic Security Perimeter(s)* (Apr. 17, 2017), https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-6.pdf.

BES Cyber Systems to do the same.[10] In Order No. 843, the Commission considered a proposal to impose a more prescriptive set of electronic access requirements for low impact BES Cyber Systems, modelled on the requirements for high and medium impact BES Cyber Systems. Instead of adopting that proposal, it accepted CIP-003-7 that allowed for ten different conceptual frameworks for achieving the security objective of allowing only necessary inbound and outbound electronic access.[11] The Commission directed NERC to assess, after eighteen months, how low impact BES Cyber Systems were implementing electronic access controls. In its resulting study report on the implementation of CIP-003-7, NERC found that registered entities use a variety of methods of electronic access controls, including firewalls, routers, uni-directional gateways, and physical isolation.[12] NERC also found that "many registered entities implemented a defense in depth model to add extra layers of protection to the assets containing low impact BES Cyber Systems."[13] Ultimately, NERC concluded that the electronic access controls generally provide an adequate level of security.[14]

In short, the Commission wisely permitted low impact BES Cyber Systems to use diverse methods to control electronic access, and the result has proven effective. Changing course now to impose a one-size-fits-all INSM requirement for low, medium,

---

[10] *Revised Critical Infrastructure Prot. Reliability Standard CIP-003-7 – Cyber Security – Security Mgmt. Controls*, Order No. 843, 163 FERC ¶ 61,032, P 3 (2018).

[11] *Id.*

[12] NERC, CIP-003-8 Electronic Access Controls Study 1 (Jun. 30, 2021), No. RM17-11-000, eLibrary No. 20210630-5159.

[13] *Id.* at 3.

[14] *Id.* at 9.

and high impact BES Cyber Systems would be inconsistent with the Commission's successful approach so far.

3. Expanding INSM to low impact BES Cyber Systems would impose a significant cost burden.

The sheer number of low impact BES Cyber Systems will impose a significant cost burden. Approximately 87% of BES locations contain low impact BES Cyber Systems.[15] Thus, expanding any INSM requirement to low impact BES Cyber Systems would result in a nearly eight-fold increase in the locations being monitored. And that increase is just the tip of the iceberg.

The high costs of implementing INSM even on simple networks containing high and medium impact BES Cyber Systems is well-known. Establishing a baseline of "normal" internal network traffic is labor intensive, and because the baseline must be re-established after any change on the system, baselining costs are not just one-time startup costs, but rather ongoing costs. Monitoring and detecting unauthorized activity is similarly labor intensive and costly. Not all deviations from the baseline are unauthorized activity, so each deviation must be investigated to determine the underlying cause (potentially resulting in re-establishing the baseline or having to modify the monitoring criteria). Finally, packet capture requires costly investment to store massive amounts of data.

But those high costs are even greater for low impact BES Cyber Systems. A high or medium impact BES Cyber System at a control center is typically centralized and geographically compact with few devices within its electronic security perimeter; in

---

[15] Supply Chain Risk Assessment at 7.

contrast, a low impact BES Cyber System on a large wind farm could include many devices spread over a large network using multiple communication protocols. Implementing INSM on the latter network is much more difficult and costly: developing the baseline is an order of magnitude more complex, monitoring involves many more deviations from the baseline, and the amount of packet capture data is exponentially greater. One TAPS member has determined that it would cost between $250,000-$500,000 to implement a solution to capture its small amount of network traffic for only 30 days.

In sum: implementing INSM costs is particularly costly for each low impact BES Cyber System, and there are far more low impact BES Cyber Systems. Given the significant costs of and technical barriers, and the comparatively lower benefit to BES reliability, of expanding the NOPR's proposed directive to include low impact BES Cyber Systems, the Commission should not do so.

B. NERC has multiple tools, other than standards, that could be more effective at achieving the reliability object as to low impact BES Cyber Systems.

Instead of allocating resources to developing a new or modified standard for requiring INSM for low impact BES Cyber Systems, NERC can more effectively support the security and reliability of the grid using its existing tools, including guidelines, technical bulletins, and alerts. As an initial matter, NERC is already developing revisions to CIP-003-8 that takes steps towards detecting malicious actions on low impact BES Cyber Systems: Project 2020-03 – Supply Chain Low Impact Revisions 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."[16] The current draft standard suggests that one way to satisfy its requirements is to use intrusion detection systems,[17] which is one of the same tools used to implement INSM.[18]

But NERC's cybersecurity efforts go far beyond developing new reliability standards. NERC has the ability to issue Alerts, which can be used to address rapidly evolving cyber threats, and identify recommended or essential mitigation actions.[19] NERC has issued dozens of Alerts to the industry, the majority of which are related to cybersecurity.[20] Most recently, NERC issued an Industry Recommendation entitled "Preparation for Potential Russian Cyber Activity against Industry from Russia-linked Actors – Level II."[21] The Alert process demonstrates that NERC, in coordination with federal government partners, can issue timely recommendations on current cyber threats.

In addition, NERC's guidelines and technical bulletins can assist owners and operators of low impact BES Cyber Systems in protecting against cyber threats. Last year's practice guide on network monitoring sensors raised awareness of certain INSM components and provided clarity on how such technology could be implemented in a

---

[16] NERC, *Standard Authorization Request (SAR)* 1-2 (Mar. 18, 2020), https://www.nerc.com/pa/Stand/202003_Supply_Chain_Low_Impact_Revisions_DL/2020-03_Supply_Chain_LIR_SAR_04032020.pdf.

[17] NERC, *CIP-003-X - Cyber Security — Security Management Controls* (Apr. 8, 2020), https://www.nerc.com/pa/Stand/202003_Supply_Chain_Low_Impact_Revisions_DL/2020-03_Supply_Chain_Lows_CIP-003-X_clean_02252022.pdf.

[18] NOPR P 9.

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

[20] NERC, *Alerts*, https://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx (last accessed Mar. 22, 2022).

[21] *Id.*, 2022 Alerts (Feb. 15, 2022).

manner consistent with the existing standards.[22] And the previous year, NERC staff and Commission staff jointly 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.[23]

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. NERC's other tools can be more effective for some of those risks.

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 necessary to address the identified threats to low impact BES Cyber Systems.

---

[22] NERC, *ERO Enterprise CMEP Practice Guide, Network Monitoring Sensors, Centralized Collectors, and Information Sharing* (Jun. 4, 2021), https://www nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf.

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

C. Further study is needed before applying INSM to a subset of low impact systems.

The NOPR asks whether there is an identifiable subset of low impact BES Cyber Systems to which INSM requirements should apply.[24] As discussed above, the answer to that question is no. But if the Commission nevertheless directs NERC to develop a new or modified standard to require INSM for a subset of low impact BES Cyber Systems, the Commission should defer to NERC's technical expertise in identifying that subset and provide adequate time for NERC to study an appropriate, risk-based subdivision of the low impact category.

TAPS acknowledges that, within the low impact category, some BES Cyber Systems pose more reliability risk than others. For example, BES Cyber Systems associated with a 25 MW generator and a 1,499 MW generator are both considered low impact, though the potential impact to grid reliability is obviously greater for the larger generator. But subdividing the low impact category is more complex than simply changing voltage or MW thresholds for the existing categories.

Any subdivision of the low impact category should be risk-based, so that the mitigation is tailored to the identified risks. There are many potential dimensions for subdividing low impacts: by function (e.g., control center, blackstart generation, etc.); by capability (e.g., external routable connectivity); by risk factors (e.g., unsupervised vendor remote access). NERC has already collected some data that might be helpful in informing

---

[24] NOPR P 34.

how to subdivide the low impact category,[25] but more analysis and data collection is needed before any conclusions could be drawn.

TAPS understands that NERC is already taking actions to further that objective. The NERC Board of Trustees issued a resolution in 2020 to initiate a project to require certain supply chain protection for low impact BES Cyber Systems and to require NERC staff to report every six months on the effectiveness and sufficiency of the supply chain standards, including identification of further actions.[26] And in February 2021, the NERC Board of Trustees further resolved that NERC staff, in coordination with stakeholders, should expeditiously complete their review and analysis of the degrees of risk presented by various low impact BES Cyber Systems.[27] Pursuant to those resolutions, NERC's Reliability and Security Technical Committee surveyed registered entities in the fall of 2021, and plans to present the results to the NERC Board of Trustees in May 2022 along with any potential next steps.[28]

Given that NERC is already analyzing issues closely related to the NOPR's question about a potential subset of low impact BES Cyber Systems to which INSM requirements should apply, the Commission should allow NERC to continue those efforts rather than issuing a directive at this time.

---

[25] Supply Chain Risk Assessment at 2-3.

[26] NERC, *Resolution for Agenda Item 8.d: Supply Chain Recommendations* (Feb. 6, 2020), https://www nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Approved_Resolution_%20Supply%20Chain%20Follow%20Up%20(2-6-2020).pdf.

[27] NERC, *Board of Trustees Minutes*, at 7 (Feb. 4. 2021), https://www nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Minutes%20-%20BOT%20Open%20-%20Feb%204%202021.pdf.

[28] NERC, *Reliability and Security Technical Committee Agenda* (Mar. 8, 2022), https://www.nerc.com/comm/RSTC/AgendaHighlightsandMinutes/RSTC_Meeting_March_8_2022_Agenda_Package_ATTENDEE.pdf.

Postponing any directive regarding INSM for a subset of low impact BES Cyber Systems will provide the additional benefit of allowing the Commission, NERC, and the industry to benefit from lessons learned resulting from any final rule issued in this proceeding. As discussed above, implementing INSM is a complex endeavor, and is even more highly complex for low impact BES Cyber Systems. Requiring high and medium impact BES Cyber Systems to implement INSM first would provide the industry adequate experience to, at a later date, evaluate whether and how to implement INSM for a subset of low impact BES Cyber Systems.

CONCLUSION

For the reasons described above, the Commission should *not* extend the NOPR by directing NERC to develop a standard requiring implementation of INSM on low impact BES Cyber Systems.

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

March 28, 2022