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 EDISON ELECTRIC INSTITUTE, THE AMERICAN PUBLIC POWER ASSOCIATION, THE LARGE PUBLIC POWER COUNCIL, THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, AND THE ELECTRIC POWER SUPPLY ASSOCIATION

The Edison Electric Institute ("EEI"), the American Public Power Association ("APPA"), the Large Public Power Council ("LPPC"), the National Rural Electric Cooperative Association ("NRECA"), and the Electric Power Supply Association ("EPSA")(together, the "Trade Associations") submit comments in response to the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("Commission") on January 20, 2022, in the above-captioned docket.[1] The Commission seeks comments on its proposal to direct the North American Electric Reliability Corporation ("NERC"), the Commission-certified Electric Reliability Organization ("ERO"), to develop new or modified Reliability Standards that would require network security monitoring internal to a Critical Infrastructure Protection ("CIP") networked environment (known as internal network security monitoring or "INSM") for high- and medium-impact Bulk Electric System Cyber Systems ("BES Cyber Systems").

The Trade Associations agree with the Commission that the implementation of INSM in some form may improve the security posture of responsible entities owning or operating high-impact BES Cyber Systems, for the reasons discussed below. However, there are significant

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, 178 FERC ¶ 61,038 (2022)("NOPR").

obstacles to the near-term implementation of this technology. Forms of INSM are in their infancy, only now being utilized by a relatively small group of utilities, and the necessary technology is not widely available. There is a limited group of subject matter experts ("SMEs") capable of working with the technology. Further, related processes associated with the application of the technology (particularly, "baselining" existing network traffic and "packet capture" and analysis) are expected to be challenging, and consensus concerning best practices has not yet been reached.

For these reasons, before issuing any directive, the Trade Associations ask the Commission to convene a forum in which Commission staff, stakeholders and knowledgeable SMEs, and NERC staff may discuss the issues described herein and exchange information on the state and availability of existing technology, as well as its cost and efficacy. This discussion could help inform decisions regarding the most effective ways to deploy INSM for high-impact BES Cyber Systems, while also assessing the potential benefits and challenges of applying INSM requirements to all medium-impact BES Cyber Systems, for which INSM is likely to have limited utility. The discussion could also include how to accomplish the security objectives the Commission seeks to achieve using the INSM tool given the rapidly evolving market for cybersecurity tools. Following this discussion, and assuming the Commission moves ahead with a directive, the Trade Associations ask that it be limited to high-impact BES Cyber Systems and medium-impact BES Cyber Systems at control centers for now.

Finally, Trade Associations respectfully submit that use of INSM for low-impact BES Cyber Systems is unlikely to be practicable, would increase rather than mitigate risk to the BES, and would not be cost-effective from a BES reliability perspective. Accordingly, any

directive issued by the Commission should not extend to low-impact assets, or to any subset thereof.

I. BACKGROUND

A. The Trade Associations

EEI is the association that represents all U.S. investor-owned electric companies. EEI members provide electricity for about 220 million Americans and operate in all 50 states and the District of Columbia. Collectively, the electric power industry supports more than 7 million jobs in communities across the United States. EEI's members are committed to providing affordable and reliable electricity to customers now and in the future. EEI's members include generator owners and operators, transmission owners and operators and other entities that are subject to the mandatory Reliability Standards developed and enforced by NERC, the Regional Entities, and the Commission.

APPA is the national service organization representing the interests of not-for-profit, state, municipal, and other locally owned electric utilities in the United States. More than 2,000 public power systems provide over 15 percent of all kilowatt-hours sales to ultimate customers in the United States, and serve over 49 million people, doing business in every state except Hawaii. Over 240 public power utilities are registered entities subject to compliance with mandatory NERC Reliability Standards.

LPPC is the association of the 27 largest state-owned and municipal utilities in the nation. LPPC's members are located throughout the nation, both within and outside the boundaries of regional transmission organizations and independent system operators. The members comprise the larger asset-owning utilities in the public power community, owning approximately 90 percent of the transmission assets owned by non-federal public power entities. LPPC members

are also members of APPA.

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are built by and owned by the people that they serve and comprise a unique sector of the electric industry. Electric cooperatives operate at cost and without a profit incentive. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landmass.

EPSA is the national trade association representing competitive power suppliers in the U.S. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. EPSA seeks to bring the benefits of competition to all power customers. This pleading represents the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

B. The NOPR

The Commission proposes to direct NERC to develop new or modified CIP Reliability Standards requiring that applicable entities implement INSM for their high- and medium-impact BES Cyber Systems. The Commission asserts that INSM could better position an entity to detect malicious activity that has circumvented perimeter controls. The Commission maintains that, because an attacker that moves among devices internal to a trust zone must use network pathways and required protocols to send malicious communications, INSM will potentially alert an entity to the attack and improve the entity's ability to stop the attack at its early phases.[2] By providing visibility of network traffic that may only traverse internally within a trust zone, INSM may warn entities of an attack in progress. The Commission offers that INSM could also be used

[2] NOPR at P 11.

to record network traffic for analysis, providing a baseline that an entity could use to better detect malicious activity. Establishing baseline network traffic allows entities to define what is and is not normal or expected network activity and determine whether observed anomalous activity warrants further investigation.[3] According to the Commission, INSM could improve the posture of an entity to detect the early phases of an attack and reduces the likelihood that an attacker could gain a strong foothold and potential command and control, including operational control, on the target system as well as potentially improve incident response by providing higher quality data about the extent of an attack internal to a trust zone. The Commission states that the new requirements should address the following three security objectives for each responsible entity:

(1) development of a baseline for their network traffic by analyzing expected network traffic and data flows for security purposes. The Commission asserts that this objective reduces the likelihood that an attacker could exploit legitimate cyber resources to: (1) escalate privileges, i.e., exploit a software vulnerability to gain administrator account privileges; (2) move undetected inside a CIP networked environment (i.e., trust zone); and (3) execute unauthorized code.[4]

(2) the ability to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP networked environment (i.e., trust zone). This objective would be to reduce detection time, which shortens the time an attacker has to leverage compromised user accounts and traverse unmonitored network connections.[5]

---

[3] *Id.* at P 12.

[4] *Id.* at P 31.

[5] *Id.*

(3) support operations and response by requiring responsible entities to log and packet capture network traffic; maintain sufficient records to support incident investigation (i.e., monitoring, collecting, and analyzing current and historical evidence); and implement measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. The Commission claims that logging, including packet capture, of network traffic is critical for a responsible entity to assess the severity of an attack, assess the scope of systems compromised, and devise appropriate mitigations.[6]

The Commission seeks comments on all aspects of the NOPR particularly asking: (1) the potential challenges to implementing INSM (e.g., cost, availability of specialized resources, and documenting compliance); (2) the appropriate capabilities (e.g., software, hardware, staff, and services) are appropriate for INSM to meet the security objectives described above; (3) the sufficiency of the proposed security objectives and, if not sufficient, the other pertinent objectives that would support the overarching goal of having responsible entities successfully implement INSM; and, (4) a reasonable timeframe for expeditiously developing and implementing Reliability Standards for INSM.[7]

While the focus of the NOPR is on high- and medium-impact BES Cyber Systems, the Commission also seeks comment on the usefulness and practicality of implementing INSM to detect malicious activity in networks with low-impact BES Cyber Systems, including any potential benefits, technical barriers and associated costs. In particular, the Commission seeks

[6] *Id.*

[7] *Id.* at P 32.

comments on whether the same risks associated with high- and medium-impact BES Cyber Systems apply to low-impact BES Cyber Systems.[8]

II. COMMENTS

A. While Security Monitoring Can Help Detect Malicious Activity, Further Discussion and Development Are Needed Before a Directive is Issued.

The Trade Associations agree with the Commission that INSM holds significant potential to increase grid visibility and the capability of detecting and mitigating malicious activity. Trade Association members who are early adopters of INSM, those with pilot programs and others studying implementation report that INSM can help improve network and threat awareness within trust zones that host critical infrastructure and key resources. Using INSM may also help responsible entities more easily identify and protect critical dependencies between cyber systems used to operate the BES. While entities have visibility at the electronic security perimeter, they may have limited visibility inside networks due to lack of capability in signature-based methods of detection, as well as inability to synthesize data in ways that INSM promises. Timely and accurate alerts regarding network flows that deviate from expected patterns can help identify malicious activity early in the attack life cycle. Secure and detailed host and network logging results in a more effective way to identify the range and depth of an attack. INSM, if implemented with proper cyber technologies and focused on the assets that pose the highest risk to the BES, could result in improved visibility, early alerting and reduced response times for unexpected activities within the monitored network trust zones.

With this said, and as further discussed below, there are significant obstacles to the near-term implementation of this technology. Elements of INSM are only now being tested or used

[8] *Id.* at P 33.

by a relatively small group of utilities and the necessary technology is not widely available. Furthermore, there is a limited group of SMEs capable of working with the technology. Responding to White House Executive Order No. 14028 on Improving the Nation's Cybersecurity,[9] and the July 28, 2021, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems to comprehensively address cybersecurity for critical infrastructure,[10] the electric industry and its government partners have coordinated in developing approaches to deploying elements of INSM. But the ensuing deployments are at a relatively early stage, and the results still being studied. Neither the technology nor the personnel needed to administer it are yet widely available.

Further, an objective, prioritized and risk-based approach for any INSM requirements is appropriate so that entities can choose from the available tools that best fit their environments, systems, networks, and architectures. Related processes associated with the application of INSM technology described in the NOPR (particularly, "baselining" existing network traffic and "packet capture" and analysis) are expected to be costly, and agreement on best practices has not been reached. For these reasons, before issuing a directive, the Trade Associations ask the

---

[9] Executive Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021), https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[10] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, Section 2 (Industrial Control Systems Cybersecurity Initiative), (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (National Security Memorandum). *See also* The White House, *Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure*, (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ (The White House July 28, 2021 Fact Sheet).

Commission to convene a forum in which Commission staff, knowledgeable SMEs, and NERC staff may exchange information on the state and availability of existing technology, and its cost and efficacy.

B. The Trade Associations Support a Focus on High-Impact BES Cyber Systems and Medium-Impact BES Cyber Systems at Control Centers.

Potential improvements in the security posture associated with INSM, when balanced with the practical challenges to immediate widespread implementation, would support a near-term focus on implementation with respect to high-impact BES Cyber Systems identified as a High Impact Rating BES Cyber System (Reliability Standard CIP-002-5.1a Attachment 1 1.1, 1.2, 1.3, 1.4) or a control center identified as a Medium Impact Rating BES Cyber System (CIP-002-5.1a Attachment 1 2.11,2.12,2.13). The risks associated with the consolidation of control and potential widespread impacts to the grid warrant monitoring for unauthorized local, network, and remote connections on the highest risk assets. Further, high-impact control centers have more IT-based BES Cyber Systems environments, and consequently more SMEs available to assist with security and compliance activities. Prioritizing high-impact BES Cyber Systems would also allow responsible entities and the ERO Enterprise to gather operational experience with INSM technology with respect to the assets that, if compromised, could pose the greatest risk to the reliability of the grid.

The risk associated with medium-impact BES Cyber Systems is generally lower than might be thought, since most comprise transmission and generation assets, and not control centers. Further, not all medium-impact BES Cyber Systems have external routable connectivity ("ERC"), meaning there is little attack surface and even less to monitor. This is particularly true of medium-impact BES Cyber Systems that are not at control centers, i.e., substations and generating facilities. Even within medium-impact BES Cyber Systems, those

without ERC do not contain the same risk (or potential impact) as those with it because an attacker does not have a path to move beyond the local trust zone. For example, a substation may only have firmware devices with code that look at sensors on a line which do not have an operating system, rendering the monitoring of the end device of little value.

If standards as proposed were to apply to all medium-impact BES Cyber Systems, the footprint for monitoring and detecting unauthorized activity on devices and software for large entities with multi-state footprints could be in the range of several hundred physical locations. Implementation would likely require responsible entities to install new or upgraded network equipment, increase network connectivity between locations, and install multiple INSM monitoring devices that could need to be aggregated to provide a complete operating picture or baseline. To implement INSM across all medium-impact BES Cyber Systems simultaneously with high-impact BES Cyber Systems would stretch already limited personnel as described in more detail below with little to no additional value at assets that have no ERC. It also would be counterproductive to add ERC to lower risk systems at remote locations for the sake of monitoring because that same connection could provide a path for an attacker to move to another trust zone, thereby increasing, rather than mitigating, risk to the BES. In other words, in seeking to mitigate a potential vulnerability, a new one would be created.

Limiting the implementation of INSM to BES Cyber Systems identified as a High Impact Rating BES Cyber System (Reliability Standard CIP-002-5.1a Attachment 1, 1.1, 1.2, 1.3, 1.4) or a control center identified as a Medium Impact Rating BES Cyber System (CIP-002-5.1a Attachment 1, 2.11, 2.12, 2.13) would help focus limited resources most effectively, consistent with the design of the current CIP standards, notably CIP-005 R1 and Part 1.5, which recognize the higher risk profile of medium-impact control centers as compared to the larger

group of medium-impact BES Cyber Systems. Requirement R1 requires responsible entities to "implement one or more documented processes that collectively include each of the applicable requirement parts in in CIP-005-6 Table R1." Table R1, Part 1.5 requires the process for "Electronic Access Points for High Impact BES Cyber Systems" and "Electronic Access Points for Medium Impact BES Cyber Systems *at Control Centers*" (emphasis added). The focus, when considering medium-impact BES Cyber Systems on control centers, recognizes that the respective assets have different risk profiles warranting varied treatment. This approach would appropriately align the concerns identified by the Commission with greater security risk environments, while avoiding the expense and potential missteps associated with a broader rollout of this new and still maturing technology.

For these reasons, the Trade Associations recommend that, if the Commission proceeds with a directive, the Commission focus efforts BES Cyber Systems identified as a High Impact Rating BES Cyber System (Reliability Standard CIP-002-5.1a Attachment 1, 1.1, 1.2, 1.3, 1.4) or a control center identified as a Medium Impact Rating BES Cyber System (CIP-002-5.1a Attachment 1, 2.11, 2.12, 2.13), while allowing NERC and industry to gather operational experience with INSM technology that will better inform whether to implement BES Cyber Systems in the vast range of remaining medium-impact BES Cyber Systems.

C. Technical Barriers and Challenges to Implementing INSM Favor a Phased Approach.

The Commission specifically asks:

> (1) what are the potential challenges to implementing INSM (e.g., cost, availability of specialized resources, and documenting compliance); (2) what capabilities (e.g., software, hardware, staff, and services) are appropriate for INSM to meet the security objectives described [in the NOPR]; (3) are the security objectives for INSM…necessary and sufficient and, if not sufficient, what are other pertinent objectives that would support the goal of a having responsible entities successfully implement INSM; and (4) what is a reasonable timeframe for

> expeditiously developing and implementing Reliability Standards for INSM.[11]

The challenges to full implementation of INSM at this time are significant. There are few vendors available to assist in providing this capability. Further, because the technology is so new, personnel with expertise in its implementation are in short supply, and availability of the technology has been hampered by supply chain delays. For closely related reasons, each application of this technology is costly and potentially would distract responsible entities from other cybersecurity, reliability-related functions.

In addition, a number of the concepts described in the NOPR merit further consideration and development. The meaning and proposed scope of "baselining," as used in this context, and full "packet capture" are not fully defined, posing a significant challenge to their immediate implementation in a dynamic and rapidly evolving market for operational technology ("OT"). Objective standards with reasonable latitude and flexibility for responsible entities to define a monitoring program that would adequately implement and operationalize INSM technology according to the risk posture of individual companies' BES Cyber Systems and related systems is a key piece of determining whether and how to use INSM.

While there are benefits to INSM requirements, the security objectives described by the Commission must be evaluated and balanced in light of technical feasibility, resource requirements and availability, implementation costs and a workable framework for compliance. Trade Associations respectfully submit that the challenges of implementing INSM justify the measured, phased approach to deployment proposed above. Below are the Trade Associations' comments on the Commission's three identified security objectives.

[11] NOPR at P 32.

1. Security Objective No. 1: Baselining Legitimate Network Traffic

The Commission states that the new CIP requirements should require responsible entities to develop a baseline for their network traffic by analyzing expected network traffic and data flows for security purposes. The Commission asserts that baselining reduces the likelihood that an attacker could exploit legitimate cyber resources to: (1) escalate privileges; (2) move inside a trust zone; and (3) execute unauthorized code. The Commission notes that the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology have recommended detailed cybersecurity practices, which include elements of INSM, such as recommending that organizations conduct network baseline analysis on control systems and networks to understand approved communication flows and to monitor control systems for malicious activity on control systems.[12]

The Trade Associations agree that, conceptually, a baseline offers the potential to reduce the likelihood that an attacker could exploit legitimate cyber resources and remain undetected. The effectiveness of an INSM infrastructure to alert security personnel about adversarial activity depends heavily on effective initial and ongoing baselining of activity on the BES Cyber Systems in question.

Nonetheless, establishing a baseline of legitimate network traffic is challenging and calls for significant judgments unique to the implementation of INSM, not all of which have yet been thought through. Trade Association members who have experience with INSM in connection with high-impact assets have discovered that baselining can have many different meanings. Baselining could mean simply understanding and differentiating between alerts that are false

[12] NOPR at P 31.

positives as opposed to actual malicious activity. Baselining could also mean having a full map of every packet between every asset on a network. To help address these issues, the Trade Associations suggest that the Commission open a discussion with affected stakeholders and Commission and NERC staff in the context of the meeting we have recommended above, with the aim of developing a workable definition. Having a definition for a provable baseline, including where and what the boundary would be for INSM, are foundational matters that warrant discussion by experts so that registered entities can be confident that they can produce adequate, auditable evidence.

Further, as reported by Trade Association member SMEs, before INSM can be successful, responsible entities will need to install appropriate technology to monitor regular patterns of network communication and subsequently identify irregular patterns. Establishing a baseline for what is deemed to be "normal behavior" in an internal network will have different meanings to different companies, experts, and auditors.

Baselining presents additional challenges. Baselining of traffic flows is not supported in all intrusion detection systems and intrusion prevention systems products. Baselining of traffic flows requires determining what normal network traffic looks like so abnormal traffic can be detected. This takes both IT and OT personnel familiar with the equipment installed in the network and documentation of the traffic each produces. This process of baselining and corresponding adjustments is extraordinarily time consuming. To detect malicious traffic in EMS environments, entities use attack profiles that are continually refined to flag suspicious traffic and selectively capture relevant data associated to the alert for further human analysis. This level of finetuning and analysis requires entities to hire and retain highly skilled

cybersecurity SMEs to continually update attack profiles to stay current with the constantly evolving techniques of malicious actors.

The Trade Associations emphasize that the overhead to support the initiation of a baseline and its maintenance is significant. The adoption of an expansive definition for baselining, when applied to every network device without a risk-based approach, may be both extraordinarily difficult and prohibitively expensive. To illustrate, if an entity has a substation with a large network and an array of dispersed switches, the entity may need to deploy a large number of sensors on the network. Any changes to the environment, such as a new server or workstation, would require an update to the baseline collected over time to capture the expected traffic patterns. Difficult judgment calls include those regarding the number and placement of sensors throughout a network, which would be an exercise that is costly and requires ongoing maintenance. To be useful, this technology must be overseen by an active monitoring team equipped with appropriate response plans. How well this can be achieved across a large population of segmented systems of differing technologies is an open question. This would be no small effort and one that would require prioritization of limited security personnel resources who have specialized expertise. Moving limited personnel from existing security responsibilities risks the ability to process other threat indicators as experts establish baseline metrics in the INSM space.

The Trade Associations recommend that the Commission direct NERC to conduct further research and analysis with appropriate industry and stakeholder expertise to understand response times and actual detection capabilities, to determine whether and how mitigation in the early phase of an attack would be improved.

2. Security Objective No. 2: Monitoring and Detecting Unauthorized Activity in Trust Zones

The Commission states that the new CIP requirements should address monitoring and detecting unauthorized activity, connections, devices, and software inside the CIP networked environment (i.e., trust zone) to reduce detection time. The Commission describes INSM as a subset of network security monitoring that is applied within a "trust zone." The Commission also states that INSM is a fundamental element of a "zero trust" approach and should improve the cybersecurity posture of responsible entities with high- and medium-impact BES Cyber Systems. The Commission asserts that monitoring and detection shortens the time an attacker has to leverage compromised user accounts and traverse over unmonitored network connections.[13]

The Commission's approach emphasizes that any requirements for monitoring and detecting unauthorized activity must be premised on a common understanding of the concept of "internal network" or "trust zone." A trust zone and a zero-trust environment are very different concepts and raise fundamental questions that warrant conversation between the industry, the Commission staff and NERC staff to create a workable solution. While the concept of an internal network may be synonymous with the inside of a traditional electronic security perimeter, the environment is evolving. Threats like ransomware take advantage of the intrinsic network level "east/west" trust within a perimeter, and new architecture models such as zero trust are evolving where there is no "internal network" to monitor. What to monitor in an INSM environment will need SME attention and discussion (as opposed to where to monitor), because security models must evolve as does the threat environment, potentially

[13] NOPR at P 31.

rendering requirements designed around today's technology obsolete. The concepts of "internal networks" or "trust zones" also need to account for the fact that there is not, in many cases, a flat "OT network" that can be easily monitored. For example, a generating unit may have many BES Cyber Systems and many networks per system. There can be dozens of OT networks/trust zones in even a single generating unit at a multi-unit plant location. A monitoring standard prescribed at a network level could turn into a requirement to flatten all networks and limit segmentation and encryption requirements in an effort to prove compliance. Limiting such segmentation and encryption capabilities, which themselves are valuable methods to help mitigate the impact of a cyber incident, may increase the risk to reliability.

For these reasons, the Trade Associations recommend that that the aforementioned request to hold a meeting between stakeholders, Commission staff and NERC staff also discuss the size and diversity of internal networks and the varying degrees of existing secure architectures that have implemented high degrees of network segmentation or micro-segmentation of their networks. That said, this same group should consider how to avoid discouraging larger, flatter networks that, while they are easier to monitor, lose the security benefits of containment and access control from high degrees of segmentation.

The overarching goal of the NOPR is to develop standards to monitor traffic within the internal networks established by electronic security perimeters; however, prescribing where security monitoring must occur in network topological terms may have a limited lifespan. For example, zero trust architectures are moving away from perimeter-based topologies with a goal of eliminating unauthorized "east/west" communications on an internal network and encrypting all remaining authorized sessions. Usefulness of concepts such as "inside" or "internal" will diminish over time and encryption will increase as zero trust concepts continue to evolve.

As a consequence, if the Commission proceeds with a directive for INSM standards development, the Trade Associations urge the Commission to allow for flexibility in the proposed design of the standards because network security models continue to evolve in response to the changing threat landscape and technological advancements. Without flexibility in scope (i.e., the "where" of security monitoring), entities and vendors may focus on network monitoring as opposed to security by designing and developing monitoring techniques to demonstrate compliance at the expense of more robust protection. To be clear, the Trade Associations support security monitoring, but in a way that is technically and topologically flexible so entities can monitor for security events with solutions that best fit their systems, networks, architectures, and allow for the accommodation of future technological innovation in this area.

3. Security Objective No. 3: Requirements to Log and Packet Capture Network Traffic, Incident Investigation Records Maintenance, and Measures to Minimize Removal of Evidence of Compromise

The Commission proposes that any modified standards should address the ability to support operations and response by requiring responsible entities to log and packet capture network traffic. The Commission characterizes packet capture as a process allowing information to be intercepted in real-time and stored for long term or short-term analysis, providing a network defender greater insight into activity on a network.[14]

While monitoring packets on an internal network does improve visibility into communications between networked devices, the question is whether visibility at this level increases the probability of discovering malicious activity. Packet-level monitoring, logging,

[14] *Id.*

and capture of internal network traffic without limitation raises a number of practical challenges. A mandate to monitor all internal traffic would require responsible entities to redesign network topology and evaluate and prioritize monitoring costs over other risk mitigation measures such as network segmentation. If unlimited, packet capture also would result in INSM programs producing huge volumes (potentially petabytes, i.e., one million gigabytes) of data, which would have to be stored for auditing purposes. Capturing petabytes of data across an entity's system would require thousands of hours of highly specialized, site, network, and system-specific attention, while much of this data may be of little value. For example, if an INSM tool detects a behavior between two devices communicating on the network that it had not previously seen, the behavior may be flagged as an anomaly relative to the baseline, and the INSM tool would therefore send an alert to a log or console. With an INSM standard in place, an expert with detailed operational knowledge of the site and how devices on that site's network communicate with each other, would have to investigate and evaluate whether that communication between devices was appropriate. After making that determination, the SME would then need to determine whether the communication was the result of malicious intent. While this is just one example, there could be hundreds or thousands of such alerts each day. To undertake this kind of work in a mandatory and enforceable manner, for every potentially anomalous communication across all of a responsible entity's internal networks, would be an enormous effort without necessarily providing a corresponding risk-reducing benefit.

In light of this challenge, the Trade Associations recommend that a discussion between the industry, the Commission staff and NERC staff that we describe above should also include a discussion about the appropriate scope of packet capturing of network traffic. A potentially equally effective approach would be to increase the monitoring of certain traffic that may

indicate suspicious traffic. An example of this includes monitoring and analysis of Domain Name Server activity. As a general matter, computer systems used to perform OT activities should not be communicating with systems outside of the facility. For those devices that do communicate with external systems, these communications should be known, understood and predictable.

Encrypted communication is another area that warrants further discussion. Encrypted communication is generally challenging for INSM because the contents of encrypted network traffic is not understandable without first being decrypted. The soon to be effective Reliability Standard CIP-012-1 and yet to be approved CIP-012-2 require protection of communication between control centers, which many entities currently undertake using encryption. Because this traffic could be within the scope of INSM, to effectively analyze it for this purpose would require it to be decrypted and re-encrypted, which can lead to latency. Latency is a concern, to the extent it would be introduced by decrypting and re-encrypting network traffic. How this issue is addressed will depend on the function of the tool implemented, i.e., if the device is alerting, acting as a firewall, or both.

D. Other Challenges for and Capabilities Needed to Implement INSM

The Commission seeks comment on the availability of specialized resources for implementing INSM.[15] INSM presents challenges as discussed in detail below for those that already have some form of INSM, which would be exacerbated for those that would need to stand up a new program in response to any new standards. If an entity does not have INSM capabilities, the time frame to identify a solution, acquire budgeting, procure the solution with

[15] NOPR at P 32.

today's supply chain challenges in acquiring hardware, and installation, setup, configuration, and training could be several years. These challenges are then compounded by the need to find and sustain a qualified cyber work force. SMEs who are familiar with and understand the network traffic within control networks are even less prevalent than those with expertise in standard (PC/Server) network traffic for which tools have existed for much longer.

1. Purchasing and Installing Technology and Storing Huge Quantities of Data Are Significant Challenges.

Responsible entities that would need to stand up a new INSM program will have numerous technology selection and implementation decisions to make. Installation of equipment required to monitor, or "tap" network communications could require significant upgrades to each facility, including physical space, significant additional network cabling, additional electricity, and additional cooling or environment controls. Challenges also include refining and adjusting the intrusion detection systems and intrusion prevention systems to reduce false positives in the particular environment in which they are installed. The timeframe needed just to fine-tune these systems so that actionable alerts can be easily identified is a minimum of several months depending on the size and complexity of the equipment in the network. Entities may have to install specific hardware in their energy management systems ("EMS") to aggregate the traffic so that off-the-shelf software, if used, can properly consume data to monitor all internal traffic and issue an alert on potentially malicious activity. In some EMS environments, Trade Association members have had to install costly, high-end aggregation equipment for packet capture and forwarding for analysis because the entities use 10 gigabit connections within their environment. If a responsible entity's EMS consistently captures 10 gigabits per second of internal network packet traffic and this entity was required to store all that data, it would total over 1.7 petabytes per day for one BES Cyber System. Storing this tremendous amount of data

is unrealistic due to the cost of storage. To illustrate and underscore the magnitude of the potential expense, assuming an unrealistically low storage cost of at $0.01 per gigabyte, data storage would cost $17,000 per day to store packet data for just one BES Cyber System. This means the registered entity would have to pay over $18 million over the typical three-year time between audits to demonstrate compliance on a single BES Cyber System. Even if entities had the capacity to store that amount of data, it is unlikely that they could write 10 gigabits of data per second to a storage array because the write speeds required to achieve it are not typically supported. Moreover, this amount of data would exceed some entities' entire internet bandwidth by constantly streaming the data to cloud storage, rendering cloud storage an infeasible solution. In general, companies do not try to capture all data due to the high cost of all the components, and the aforementioned inability to store the vast amounts of data (the majority of which would be legitimate normal traffic, and not evidence of malicious activity). Rather, entities analyze data at strategic points in the network through which the majority of network communication must flow. These issues are challenging enough to address in the IT environment and are compounded when trying to apply learnings from the IT environment to screening and storage of data in the OT environment.

Even leaving aside the hardware obstacles and costs, being able to sort, review and/or analyze this amount of data is a challenge that few utilities would be able to handle. The best-case scenario for most utilities would be to have the data on hand for forensic research performed by a third party. Therefore, if the Commission adopts any requirement to retain copies of network traffic, those requirements should be based on the highest risk elements, focused on the data that would be most effective in aiding in forensic investigation.

If, along with INSM implementation, there is a move toward a zero-trust architecture, resource challenges may be further increased. An INSM solution in an OT environment would need to be customized to understand substation and/or generation systems. New site engineers, operations personnel, and vendors would need to be engaged due to the baselining process associated with deployment of INSM tools. This will be a time-consuming effort that the Commission must take into account and allow to mature before a uniform requirement is imposed.

The technical and practical challenges described above represent just some of the hurdles to implementing INSM. Other issues that warrant discussion among SMEs include, but are not limited to, connectivity to/from remote locations, constraints on vendor ability to identify all makes and models of installed equipment (current generation and legacy), vendor resistance to vulnerability disclosure and the potential need for collateral upgrades to support the solution (i.e., switches, routers, backend storage, capacity increases on monitoring solutions).

2. Highly-Skilled Subject Matter Experts Are in Short Supply.

In addition to acquiring new technology, responsible entities will have to hire and retain suitable subject matter expertise to implement INSM. Both finding and hiring qualified security professionals and vendors are current challenges that can be expected to continue for the foreseeable future and finding those with industrial control system experience is a distinct challenge.[16] Existing or new employees will be needed to support the infrastructure, maintain the monitoring application, and review alerts. Qualified candidates with an understanding of

[16] A Resilient Cybersecurity Profession Charts the Path Forward, ISC^2 Cybersecurity Workforce Study, 2021 at 24-26. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

OT security and communication protocols are in particularly short supply. Trade Association members with existing INSM programs have had limited success in staffing permanent positions for maintenance of their current INSM solutions, and subject matter expertise is limited while the field is in its infancy. The variety of technologies used in the OT environment further complicates SME availability. Lack of availability of SMEs exacerbates industry efforts to build the talent pool needed to mitigate adverse security and reliability impacts that may be faced when relying on new technologies to perform critical monitoring functions.

Trade Association members have particular concerns about the ability to hire and/or retain employees with the required skill set to install, tune, manage and respond to alerts from a large base of installed internal network monitoring systems. The expertise needed to analyze traffic in substations is vastly different from a cybersecurity expert working in a more traditional IT corporate network. Both IT and OT resources with these skillsets are in acutely short supply across the utility industry and from third-party service providers. Other critical infrastructure sectors (e.g., communications, natural gas, financial services, and water) are competing for this small supply of experts as well. Any standard and implementation timeline would need to account for these challenges to ensure that responsible entities can obtain the specialized and skilled human resources needed.

3. Ongoing Supply Chain Challenges Can Be Expected to Worsen.

Vendor supply chain challenges will complicate INSM implementation. Requirements that limit options for INSM tools to specific technologies will limit competition among vendors and the supply chain for these types of monitoring tools, while putting responsible entities at risk due to reliance on a limited group of vendors. While obtaining software is typically not an issue,

acquiring hardware has become much more difficult. Basic server delivery times have ballooned during the past year. Trade Association members are also experiencing longer lead times for other computing devices. For example, certain members have seen double or triple the lead time over the past few years for securing switches, routers and firewalls from a critical vendor when certain network changes have been needed. Of course, it is well known that many computer products are currently delayed by the microchip shortage plaguing many industries. This chip shortage likely will persist further into the future until additional capacity for chip manufacturing is built. Supply chain challenges will only be further exacerbated if all responsible entities are required to implement similar INSM technologies at the same time.

E. Any Future Standard Must Have Practical, Flexible and Objective Measures for Compliance.

From a regulatory compliance standpoint, the forum proposed above with Commission and NERC staff and knowledgeable SMEs should aim to establish practical, deterministic and/or objective measures of acceptable INSM performance. Under the present regulatory structure which allows for zero defects, responsible entities will have to report every defect as a violation, and to perform formal mitigation plans for each defect. NERC and standard drafting teams are appropriately moving toward creating more objective-based requirements with progressive Violation Severity Levels. If the Commission adopts a requirement, this approach is critical in development of INSM requirements. For responsible entities to be successful in mitigating risk, the proposed standards must have flexibility that enables myriad approaches toward a common security objective.

Additionally, as noted above, depending on how packet capture is defined, INSM programs could produce large volumes (potentially petabytes) of data that would have to be stored for auditing purposes. Data retention would be prohibitively expensive if the packet

capture language used in NOPR is retained. In addition, without objective metrics for compliance, proving that a company did not fail to identify malicious activity on a network will be virtually impossible. Depending on the expectations of the ERO, providing evidence of effective network baselining also will be difficult to demonstrate to an auditor.

The output of information from INSM tools also creates heightened security concerns. If a new standard requires a responsible entity to provide packet capture, these could be used to create a virtual copy of a substation or EMS, if they were accessed by malicious actors. This issue is magnified if there is only one or even a small number of repositories that hold the network data of every important BES Cyber System, making these repositories highly valuable targets for malicious actors. In other words, such a requirement could itself become the highest risk vector for the type of malicious intelligence gathering the Commission is trying to prevent. There is no satisfactory way to redact packet captures, unlike a baseline or a network diagram where an entity can control the level of detail provided to auditors. In essence, packet captures create a copy of the devices and how they communicate to cause action in a physical world. Making packet captures available outside registered entity electronic borders, combined with the network topology of systems, exposes the finer grain detail of these systems that must be protected.

Trade Associations also note that INSM assets, depending on how they are designed and implemented, could be considered Electronic Access Control or Monitoring Systems ("EACMS"), and subject to the reliability requirements applicable to those cyber assets. Such configurations may lead to overly burdensome requirements and endorsed guidance from the ERO defining when and where an INSM may be considered an EACMS will be needed to help

those entities implementing these technologies make the best choice for their particular installations.

One possible solution to demonstrate compliance would be to show INSM installations on electronic security perimeter diagrams, configuration settings for devices that mirror network traffic to the monitoring hardware, and actual alerts and responses. It will be nearly impossible for responsible entities to demonstrate that they have captured every packet traversing a specific network, because the entity would have to show that it did not miss a packet and that the amount of traffic sent to the monitoring device did not overrun available bandwidth and subsequently get dropped without detection.

F. Implementing INSM on Low-Impact BES Cyber Systems Is Not Practical.

The Commission seeks comments on the usefulness and practicality of implementing INSM to detect malicious activity in networks with low-impact BES Cyber Systems, including any potential benefits, technical barriers, and associated costs. Reflecting the approach taken under the existing standards framework, Trade Association member companies analyze cyber assets and networks to make risk-based determinations that reflect the impact of various assets on overall risk to grid operations. Low-impact systems and networks have been classified as low as a result of the minimal impact they would have on grid operations if compromised. Trade Associations respectfully submit that applying INSM to low-impact BES Cyber Systems, even if it were feasible, would not provide a cost-effective increase in BES reliability when the relatively small risk that compromise of low-impact BES Cyber Systems poses to the grid is weighed against the very substantial (indeed, likely insurmountable) challenges to adopting INSM for low-impact assets and increase rather than mitigate risk to the BES.

As a threshold matter, there are an enormous number of low-impact systems compared to high and medium. Where a responsible entity may have hundreds of high and medium assets, the number could easily be in the thousands or tens of thousands for low-impact assets spread across a much larger geographic and network footprint. Applying INSM to such a multiplicity of assets is not feasible or practical from a human resources or financial standpoint. A requirement to monitor networks with very few devices has an even lower benefit when measured against the high costs associated with implementation and ongoing support.

From a technical standpoint, low-impact facilities have different technological constructs that would complicate any effort to adopt a general INSM requirement. In the first place, low-impact BES Cyber Systems are not currently required to establish electronic security perimeters, which raises the question of how to define the trust zones for a wide variety of low-impact assets for purposes of INSM. Moreover, many low-impact substations do not have high speed data links, and many have no external routable connectivity, often due to their locations in rural areas. Connecting these devices would in fact increase their vulnerability. In addition, low-impact facilities that do have external routable connectivity are connected using low bandwidth technologies such as microwave, radio or cell modem. Facilities without available bandwidth or low bandwidth connections will be unable to send all captured packet data to a centralized location for analysis. Monitoring network traffic at a low-impact substation without a high bandwidth connection would require additional equipment to capture the traffic and analyze it on site and then transfer the results of that analysis to a centralized location. Procuring and installing individual network monitoring, packet data storage, and support equipment at each low-impact substation will be prohibitively expensive compared to the marginal, if any, security value.

The protocols that responsible entities use at low-impact facilities differ considerably from those used in higher impact facilities like control centers, and most manufacturers only support a subset of all available protocols used by utilities. Commercial off-the shelf products may not support the protocols used by some entities in their substations, further making the monitoring of substation network traffic infeasible.

If INSM is applied to low-impact BES Cyber Systems, the current supply chain challenges will be even more pronounced, as each entity required to implement INSM would be attempting to acquire the same equipment at the same time, while also competing for SMEs and vendor expertise to assist in tailoring the INSM systems and technologies to each responsible entity's unique low-impact BES Cyber Systems infrastructure.

Leaving low-impact BES Cyber Systems outside any mandate that issues in this docket would be consistent with the intent behind CIP-002-5.1a bright-line criteria to determine impact and to identify and categorize high- and medium-impact BES Cyber Systems and assets that contain low-impact BES Cyber Systems. Low-impact BES Cyber Systems have different protections commensurate with the risk posed to the BES so that entities can focus resources on higher risk assets. There is limited security value in monitoring networks at low-impact facilities, as they have already been assessed and identified not to have a significant impact on the BES and should be treated accordingly. It is simply not feasible or cost effective to target all low-impact systems and could increase rather than mitigate risk to the BES.

III. CONCLUSION

Trade Associations appreciate the opportunity to share insights into and experience with INSM. As explained above, the considerations, benefits, risks of and impediments to using the technologies are inextricably intertwined and require thoughtful solutions that allow optionality

and flexibility regarding their implementation. The Trade Associations ask the Commission to convene a meeting in which Commission staff, stakeholders and knowledgeable SMEs, and NERC staff may discuss the issues described herein and exchange information on the state and availability of existing technology, as well as its cost and efficacy.

Respectfully submitted,

/s/
Andrea Koch
Senior Director, Reliability Policy
akoch@eei.org

Bob Stroh
Associate General Counsel, Reliability & Security
rstroh@eei.org

Edison Electric Institute
Washington, D.C. 20004
(202) 508-5000

/s/
John E. McCaffrey
Senior Regulatory Counsel

American Public Power Association
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
jmccaffrey@publicpower.org

/s/
Jonathan D. Schneider
Jonathan Trotta
STINSON LLP
1775 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com
jtrotta@stinson.com

Counsel to the

Large Public Power Council

/s/

Patricia Metro
Senior Grid Operations & Reliability Director
patti.metro@nreca.coop

Mary Ann Ralls
Senior Director, Regulatory Affairs
maryann.ralls@nreca.coop

National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-5837

/s/

Nancy Bagot
Senior Vice President
nbagot@epsa.org

Bill Zuretti
Director of Regulatory Affairs & Counsel
bzuretti@epsa.org

Electric Power Supply Association
1401 New York Avenue, NW Suite 950
Washington, D.C. 20005
(202) 628-8200

March 28, 2022