NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical Energy/Electric Infrastructure Information Has Been Redacted

January 18, 2024

Ms. Debbie-Anne Reese
Acting Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Internal Network Security Monitoring Feasibility Study Report, Docket No. RM22-3-000___

Dear Acting Secretary Reese:

Pursuant to Order No. 887 of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[1] the North American Electric Reliability Corporation ("NERC") hereby submits a report providing the results of a study to guide the implementation of internal network security monitoring ("INSM"), or other mitigation strategies, for medium impact Bulk Electric System ("BES") Cyber Systems without external routable connectivity and all low impact BES Cyber Systems ("INSM Study Report"). INSM is a type of monitoring applied within a "trust zone"[2] for early detection of malicious activity that has breached perimeter network defenses.[3] NERC completed the INSM study consistent with the FERC directive in Order No. 887 to perform a study focused on: (1) the substantive risk posed by BES Cyber Systems operating without INSM; and (2) the challenges and solutions involved in extending INSM to these BES Cyber Systems.[4]

NERC is submitting a public and non-public version of the INSM Study Report. In the public version of this submittal, NERC redacted sensitive data regarding Critical Electric Infrastructure. NERC respectfully requests that the Commission designate the redacted portions of the INSM Study Report as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with the Commission's Order No. 672, Sections 39.7(b) (4) and 388.113 of the Commission's regulations, the FAST Act, and FOIA

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021, at PP 88-91 (2023).

[2] Order No. 887, at P 2, n. 6 provides the following definition of trust zone: "The U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) defines trust zone as a 'discrete computing environment designated for information processing, storage, and/or transmission that share the rigor or robustness of the applicable security capabilities necessary to protect the traffic transiting in and out of a zone and/or the information within the zone.' CISA, *Trusted Internet Connections 3.0: Reference Architecture*, at 2 (July 2020), https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf.

[3] Currently, INSM is not required by the Critical Infrastructure Protection ("CIP") Reliability Standards, but NERC initiated a standards development project to develop requirements for INSM for high and medium impact BES Cyber Systems with External Routable Connectivity.

[4] *Id.*

1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000 | www.nerc.com

Exemptions 3 and 4, respectively.[5] The redacted portions of the INSM Study Report provide sensitive information on the locations of BES Cyber Systems. Therefore, the details provided in the redacted portions of the INSM Study Report could be useful to a person planning an attack on Critical Electric Infrastructure. As a result, the redacted portions of the INSM Study Report meet the criteria for CEII as defined in the Commission's rules as it is related to Critical Electric Infrastructure, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters. NERC requests this treatment for the redacted portions of the INSM Study Report, for the full period allowed under the Commission's regulations,[6] in the interest of security around this sensitive matter.

Respectfully submitted,

/s/ Marisa Hecht

Marisa Hecht
North American Electric Reliability Corporation
Senior Counsel
1401 H Street, NW, Suite 410
Washington, D.C. 20005
202-400-3000
marisa.hecht@nerc.net

Counsel to the North American Electric Reliability Corporation

[5] *See* 18 C.F.R. §§ 388.112 - 113; FAST Act, Pub. L. No. 114-94, § 61003, 129 Stat. 1312, 1773-1779 (2015) (codified as 16 U.S.C. § 824o-1); 5 U.S.C. §§ 552(b) (3) and (b) (4) (2018).
[6] 18 C.F.R. § 388.113(e)(1).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Internal Network Security Monitoring Feasibility Study

Feasibility of implementing INSM at locations containing low impact BES Cyber Systems and medium impact BES Cyber Systems without External Routable Connectivity

January 2024

PUBLIC VERSION

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

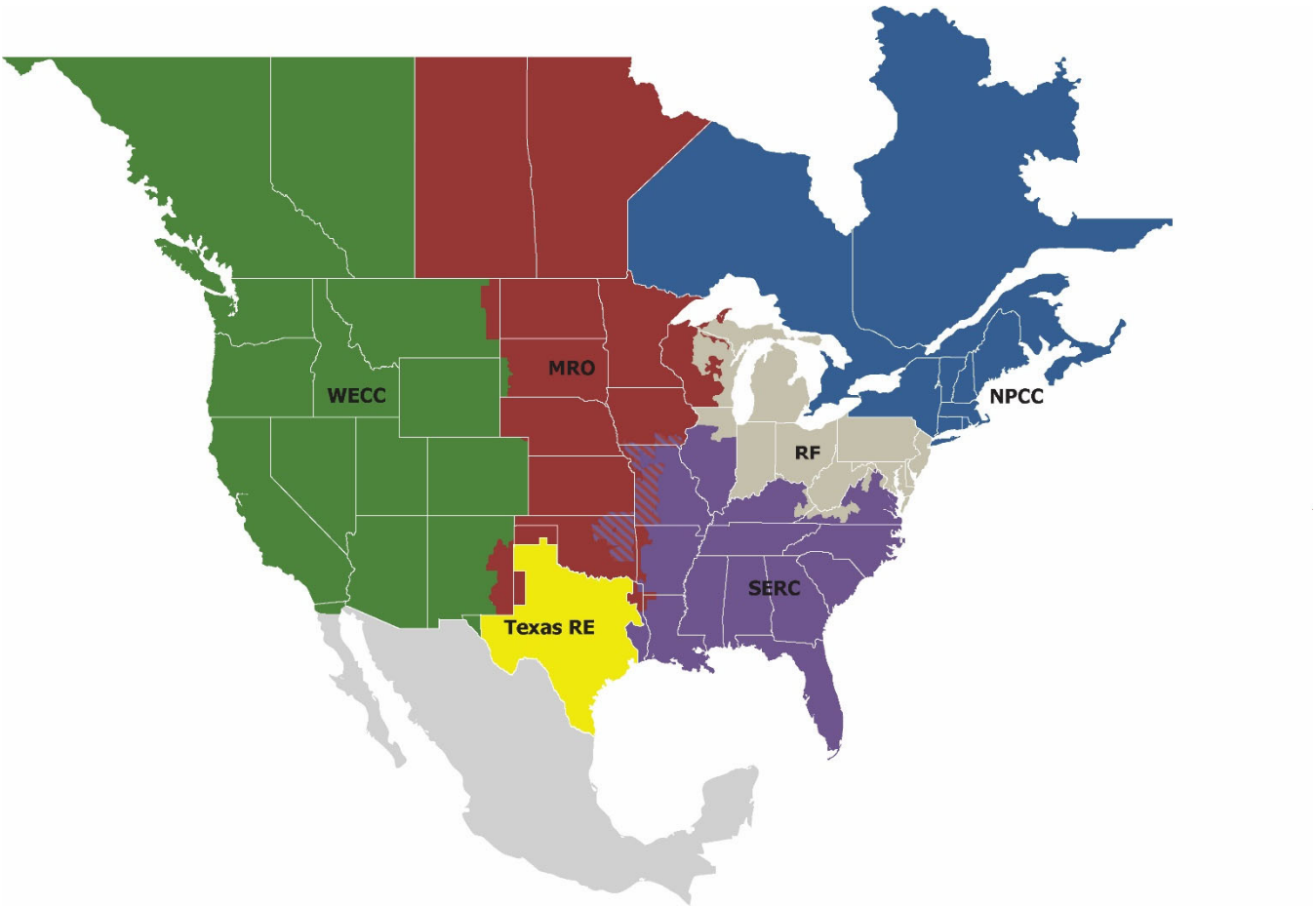
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Statement of Purpose

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887,[1] which directed the North American Electric Reliability Corporation (NERC) to submit a report, within 12 months of issuance of its final rule, that studies the feasibility of implementing Internal Network Security Monitoring (INSM)[2] at all low impact BES Cyber Systems and medium impact BES Cyber Systems without External Routable Connectivity (ERC). The following report has been developed by NERC in response to the directive and is intended to guide the future implementation of INSM, or other mitigation strategies for medium impact BES Cyber Systems without ERC and all low impact BES Cyber Systems regardless of ERC.

FERC Order No. 887 directed NERC to perform a study to support possible future Commission actions on whether to extend INSM requirements to medium impact BES Cyber Systems without ERC and all low impact BES Cyber Systems regardless of ERC status. Data collected to perform the study was used to inform an analysis regarding the substantive risks posed by these BES Cyber Systems operating without the implementation of INSM. Specifically, the order directed that the study focus on two main topics (1) risk and (2) challenges and solutions. The study is required to include a determination of:

1. ongoing risk to the reliability and security of the bulk power system (BPS) posed by low and medium impact BES Cyber Systems that would not be subject to the new or modified Reliability Standards, including the number of low and medium impact BES Cyber Systems not required to comply with the new or modified standard; and
2. potential technological or other challenges involved in extending INSM to additional BES Cyber Systems, as well as possible alternative mitigating actions to address ongoing risks.

Regarding risk FERC directed that, "… NERC should collect from registered entities information on the number of low impact and medium impact BES Cyber Systems that would not be subject to the new or revised Reliability Standards, which would inform the scope of the risk stemming from systems without INSM."[3] FERC directed that, "… NERC provide an analysis regarding the substantive risks posed by these BES Cyber Systems operating without the implementation of INSM."[4] Further, FERC directed that NERC should determine the quantity of:

1. substation and generation locations that contain medium impact BES Cyber Systems without ERC.
2. low impact locations (including a breakdown by substations, generations resources, and control centers) that contain low impact BES Cyber Systems without ERC; and
3. low impact locations that contain low impact BES Cyber Systems with ERC (including a breakdown by substations, generations resources, and control centers).

Regarding challenges and potential solutions, FERC directed that, "… NERC should identify the potential technological, logistical, or other challenges involved in extending INSM to additional BES Cyber Systems, as well as possible alternative actions to mitigate the risk posed."[5] This report fulfills these requirements and includes NERC recommendations regarding future Commission actions as it pertains to INSM requirements for the electric industry.

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (Jan. 19, 2023) [hereinafter Order No. 887].
[2] *Id.* at P 9.
[3] *Id.* at P 89.
[4] *Id*.
[5] *Id.* at P 90.

Public

Chapter 1: Internal Network Security Monitoring

FERC Order No. 887 describes INSM as follows:

> INSM is designed to address as early as possible situations where perimeter network defenses are breached by detecting intrusions and malicious activity within a trusted network zone. INSM consists of three stages: (1) collection; (2) detection; and (3) analysis. Taken together, these three stages provide the benefit of early detection and alerting of intrusions and malicious activity.[6] Some of the tools that may be used for INSM include: anti-malware; intrusion detection systems; intrusion prevention systems; [security information and event management systems;] and firewalls.[7]

INSM is primarily a detective control for monitoring east west traffic that is implemented under the assumption that attackers have already compromised the network perimeter, or the attacker is an insider with trusted network access. INSM is analogous to security personnel monitoring security cameras in the hallways and common areas of a secure building. Security personnel understand what activity is normal and are alert to anything that looks anomalous. Similarly, a properly engineered INSM solution could detect anomalous activity within a trust zone and alert cyber security personnel.

By ensuring that entities are monitoring their internal networks, compromise of a trusted third-party vendor with network access is less likely to result in a widespread successful cyber-attack by reducing the mean time to detection and facilitating faster incident response times. There are currently no standards requiring entities to monitor internal network traffic of their low impact BES Cyber System networks. Due to this, there may be little in place to detect successful intrusions into these networks, such as a compromised vendor resulting in unauthorized remote access to the low impact network. In contrast, with INSM in place, earlier detection of any malicious activity exploiting the unauthorized access is possible, thus creating a stronger opportunity to effectively reduce the impacts of a successful cyber-attack. The implementation of INSM at low impact BES Cyber Systems may also help prevent, deter, or detect lateral movement before further grid assets are compromised.

[6] *See* Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013); *see also* ISACA, *Applied Collection Framework: A Risk-Driven Approach to Cybersecurity Monitoring* (Aug. 18, 2020)
[7] Order No. 887 at P 9.

Chapter 2: Feasibility Study

In response to Order No. 887, NERC began to collaborate with representatives from the Regional Entities and began the process of conducting a study of the feasibility of implementing INSM at all low impact BES Cyber Systems and medium impact BES Cyber Systems without ERC. The team consisted of NERC staff and representatives from each of the six regional entities, see Appendix A. The following study relied heavily on the section 1600 Data Request responses, previously submitted industry comments in the Order No. 887 docket, as well as collaboration with the Electricity Information Sharing and Analysis Center (E-ISAC), and FERC additional staff.

Section 1600 Data Request

Order No. 887 directed NERC to develop Reliability Standards requirements to require INSM for all high impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with ERC. In addition, Order No. 887 directed NERC to conduct a study of the risks stemming from a lack of INSM and the feasibility of requiring it for other BES Cyber Systems not subject to the revised standards, such as low impact BES Cyber Systems and medium impact BES Cyber Systems without ERC. As part of this study, the Commission stated that NERC should collect certain information on the number of these BES Cyber Systems. The Commission directed NERC to file the study by January 18, 2024, which is within 12 months of the issuance of Order No. 887. Given the type of data and information to be collected, NERC staff acted pursuant to its authority under Section 1600 of the NERC Rules of Procedure[8]. On February 16, 2023, the NERC Board of Trustees (Board) authorized NERC staff to use expedited procedures under Section 1606 of the NERC Rules of Procedure[9] to meet the Commission directive. Consistent with the shortened procedures timeline, NERC posted the proposed data request for a 21-day comment period from March 24, 2023, through April 14, 2023. NERC provided advance notice of the posting to the FERC Office of Electric Reliability on March 8, 2023. The subsequently developed Section 1600 Data Request was reviewed by industry and approved by NERC's Board of Trustees on May 11, 2023. NERC staff issued the data request to industry on May 25, 2023. Reporting entities had 60 days to respond to the data request, which concluded on July 25, 2023. Responses were collected through the NERC ERO portal, designated confidential, and protected as such. Access to data request responses was restricted to the ERO Enterprise team performing the data analysis. The specific questions in the data request can be found in Appendix A.

Reporting Entities

Reporting entities for the INSM data request consisted of the following registered functions:

- Balancing Authorities
- Distribution Providers
- Generator Owners
- Generator Operators
- Reliability Coordinators
- Transmission Owners
- Transmission Operators
- Distribution Providers[10]

[8] NERC Rules of Procedure
[9] NERC Board of Trustees Meeting, Agenda Item 9d (Feb. 16, 2023), Board_Open_Meeting_Agenda_Package_February_16_2023.pdf
[10] Limited to Distribution Providers that have certain facilities listed in the applicability section of the NERC CIP Standards

Reporting entities responding only for a Distribution Provider (DP) that did not meet the CIP-002-5.1a applicability criteria[11] were provided an option to identify as such and opt out of the data request. This meant that at the time of the data request, these DP registered entities did not have any high, medium, or low impact BES Cyber Systems. **[REDACTED]** of the total 1,417 Reporting Entities opted out.

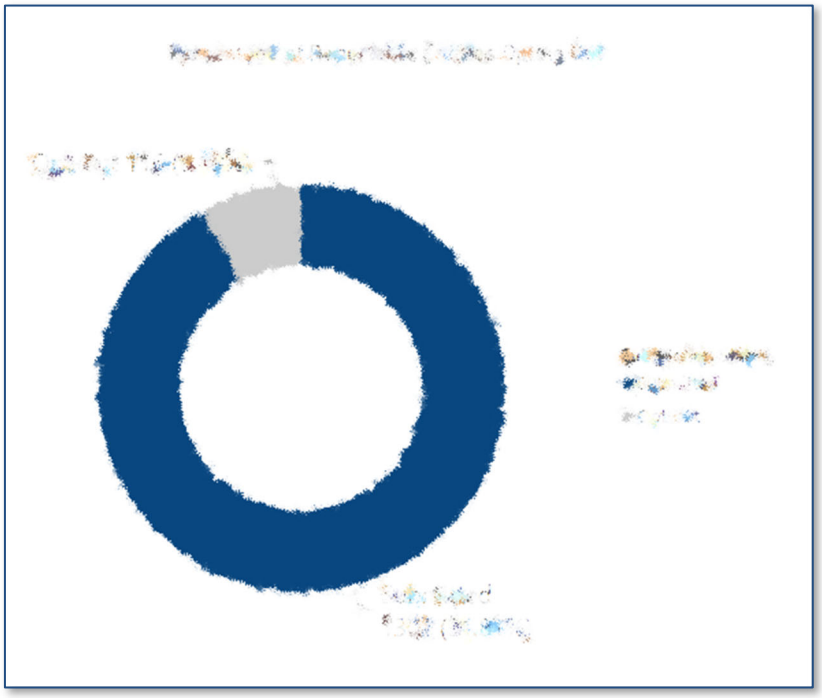


Figure 2: Percentage of Reporting Entities that Opted-out

[11] See Applicability Criteria Pg. 2 CIP-002-5.1a.pdf

Chapter 3: Analysis of Data Request Responses

Reporting entities were asked a series of ten questions (See Appendix A). Most questions were mandatory and included an option to comment. Below is a statistical analysis of responses.

Locations by Type and Impact Categorizations

Analysis of the reported BES locations, as shown in Figure 3, allows several key observations to be made:
[REDACTED]

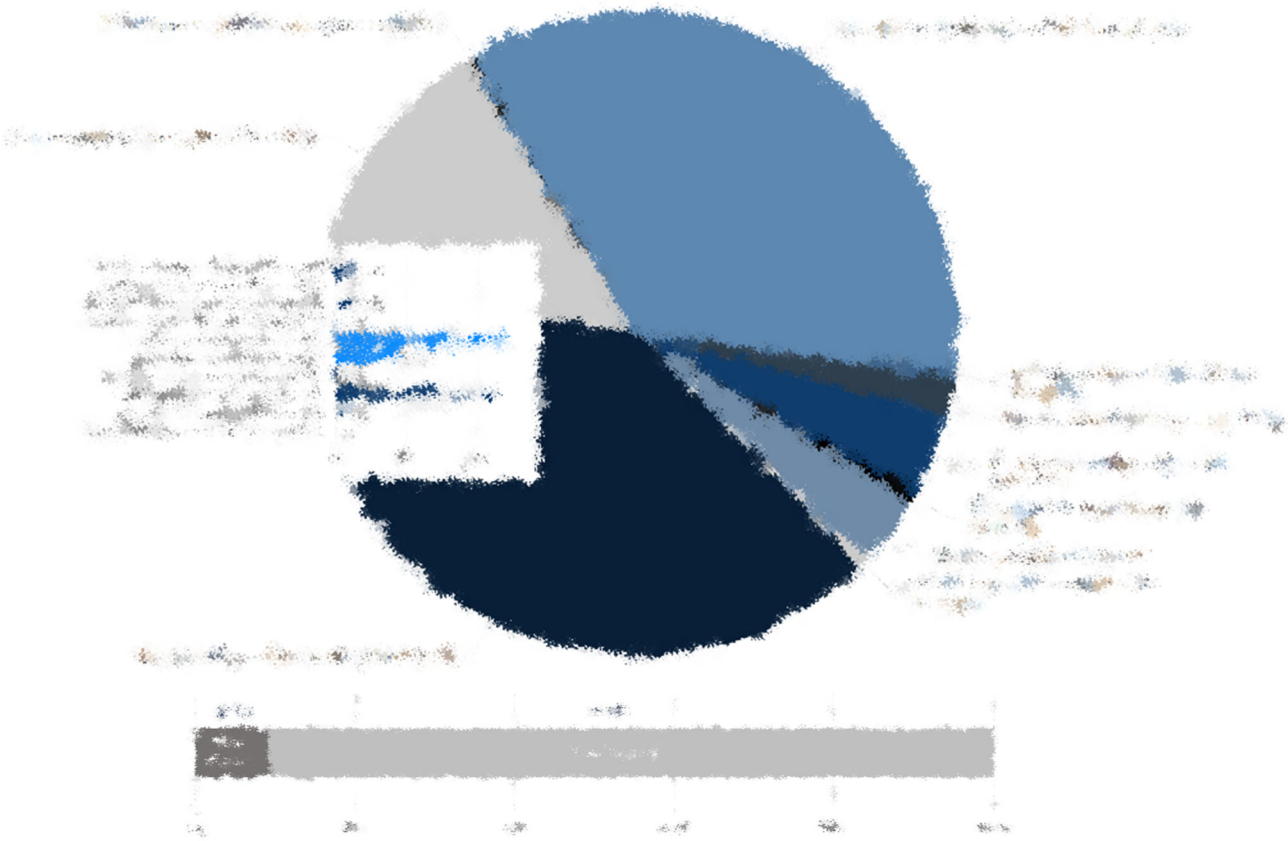


Figure 3: Locations by Impact, Function, and Connectivity

Low Impact BES Cyber System Networks

Respondents were asked to provide the estimated percentages of network configurations for their low impact BES Cyber Systems. **[REDACTED]**

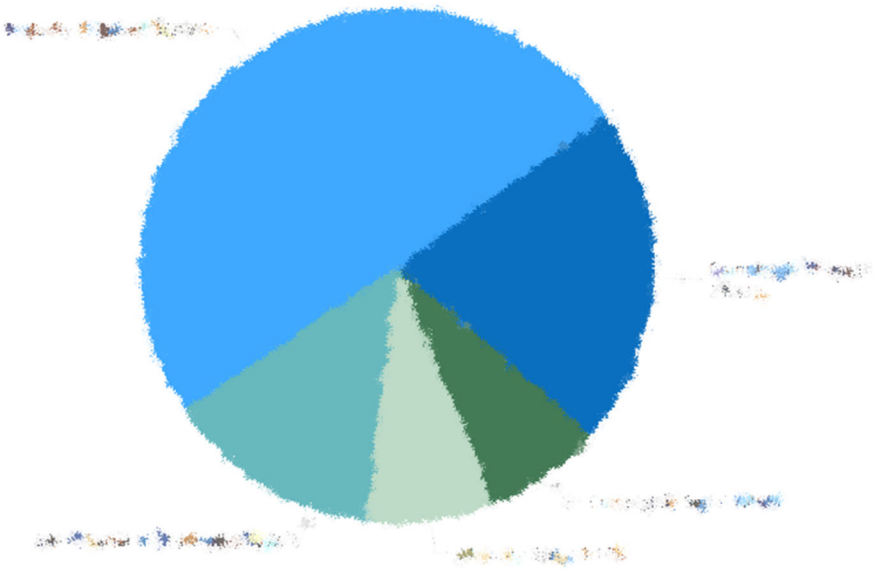


Figure 3.1: Low Impact Network Topography by Response

However, not all respondents have the same number of locations containing low impact BES Cyber Systems. Some entities have many locations, while others have only a few. If a hypothetical entity has 200 low impact locations and has responded to say that seventy-five percent of their low impact locations are completely serial while twenty-five percent are completely IP; then, by interpolation, the entity has 150 low impact locations that that are completely serial and fifty locations that are completely IP. Figure 3.2 shows what the percentages look like when all entities are considered in this way. Essentially larger entities get a compounding effect because they have more locations. **[REDACTED]**

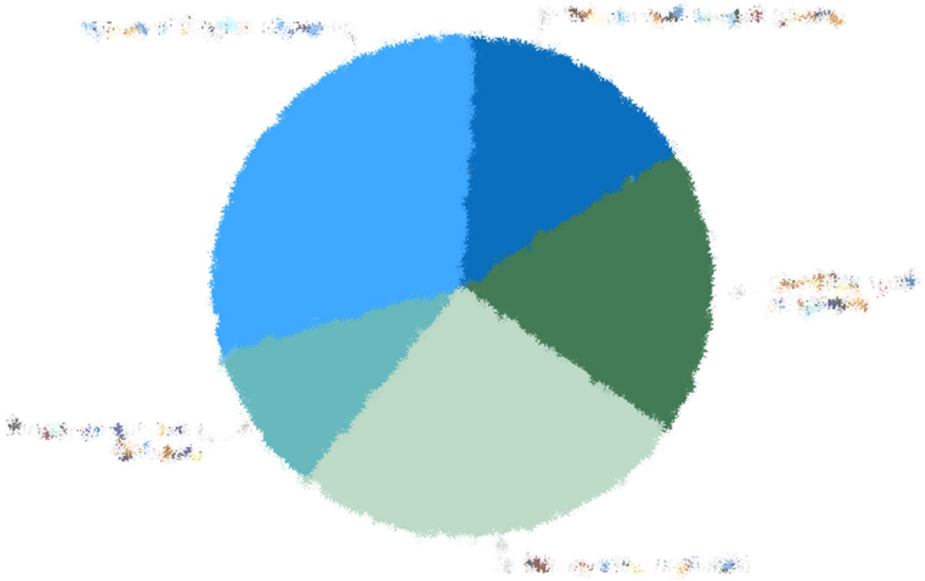


Figure 3.2: Low Impact Network Topography by Location

When sizing the respondent organizations by numbers of reported asset locations, the distribution of assets by organization sizes within the industry becomes apparent. **[REDACTED]**

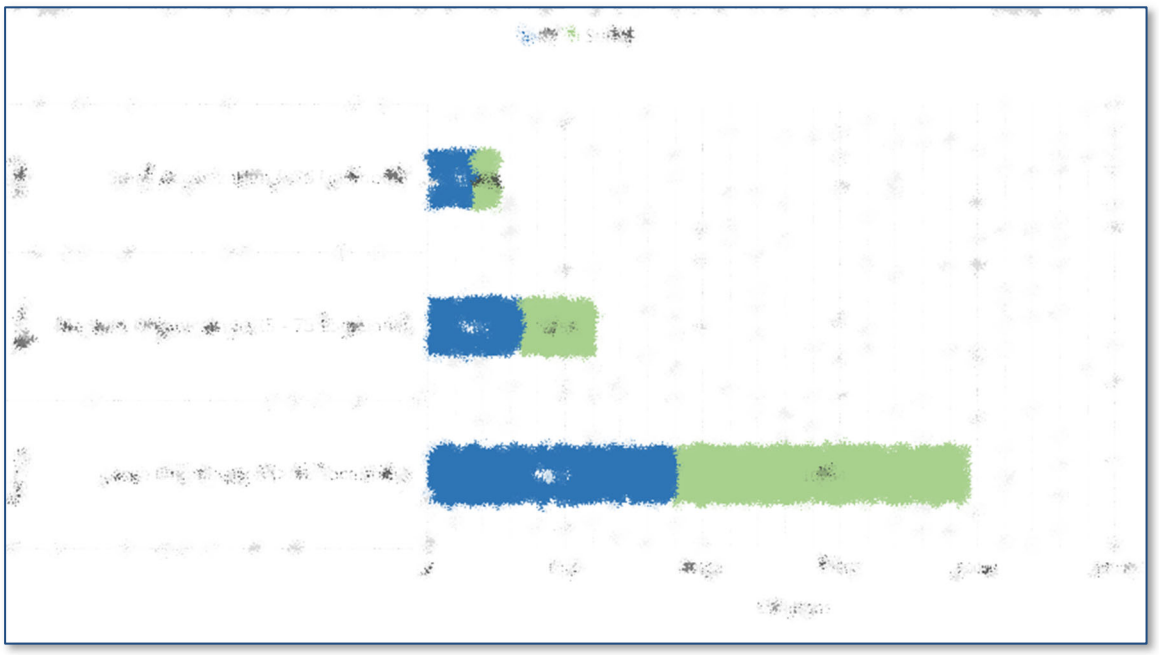
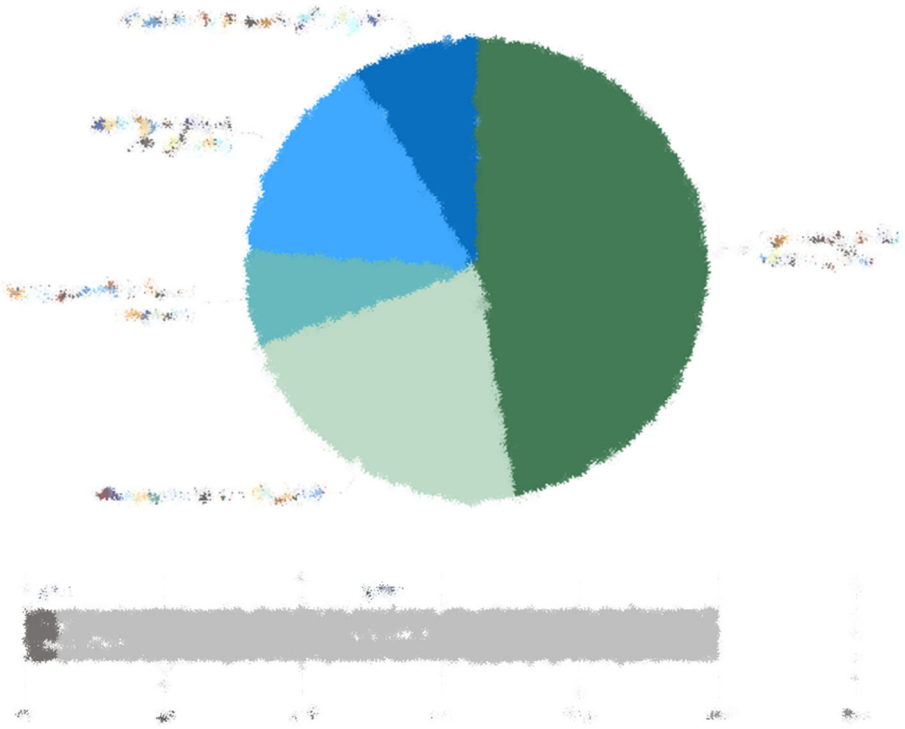


Figure 3.3: Low Impact Network Topography by Organization Size

Medium Impact BES Cyber Systems Networks (without ERC)

Reporting entities were asked to provide the estimated percentages, totaling 100% of network configurations for their locations containing medium impact BES Cyber Systems without ERC, see Figure 3.4. **[REDACTED]**

Figure 3.4: Medium Impact Network Topography by Response



[REDACTED]

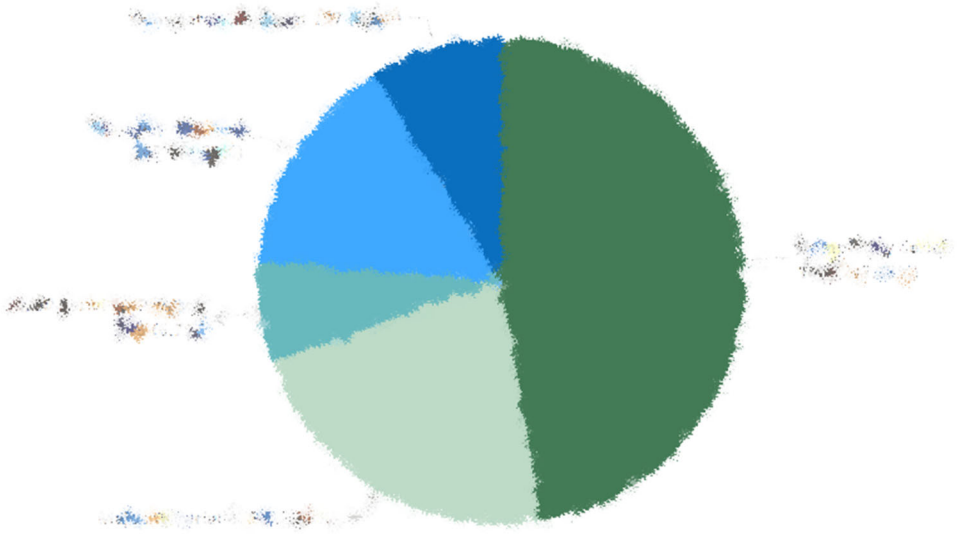


Figure 3.5: Medium Impact Network Topography by Location

Challenges Associated with Implementing INSM

Respondents were asked to independently rate each of the listed potential technological, logistical, or other challenges involved in extending INSM to additional medium impact BES Cyber Systems (e.g., medium impact without ERC) and low impact BES Cyber Systems (e.g., all low impact) using a scale of (1) least challenging to (5) most challenging. **[REDACTED]**

Figure 3.6: Challenge Ratings for Low Impact Locations

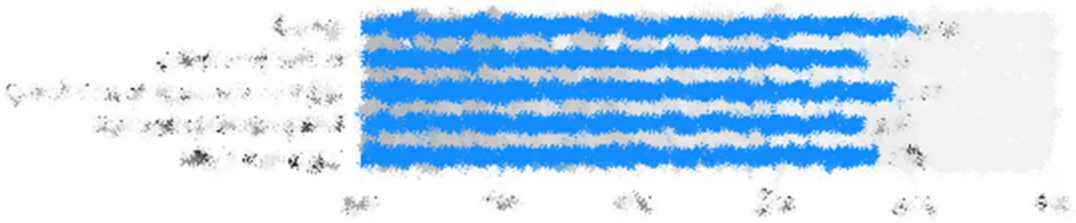


Figure 3.7: Challenge Ratings for Medium Impact Locations without ERC

Low Impact Locations with Network-Based Malicious Code Detection

Respondents were asked to provide the estimated percentage of low impact BES Cyber Systems that currently have network-based malicious code detection. Figure 3.8 shows **[REDACTED]**

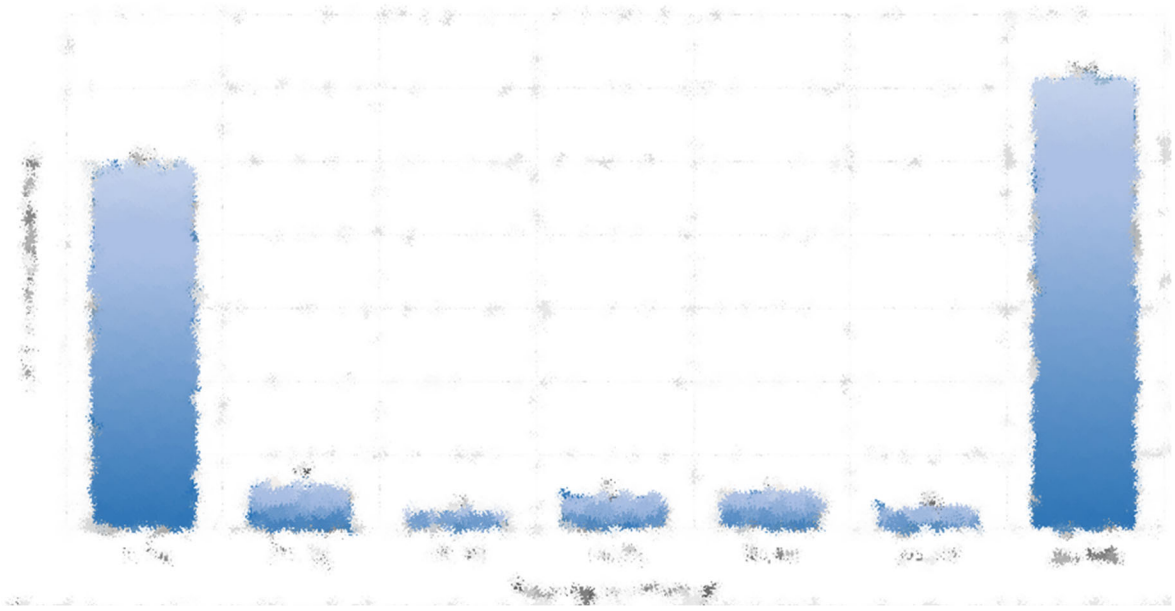


Figure 3.8: Percentage of Low Impact BES Cyber Systems with Malicious Code Detection

IP-Based Attack Surface Area by Organization Size

The data presents a couple unique insights when organization size, asset ownership, and network configurations are analyzed together. **[REDACTED]**

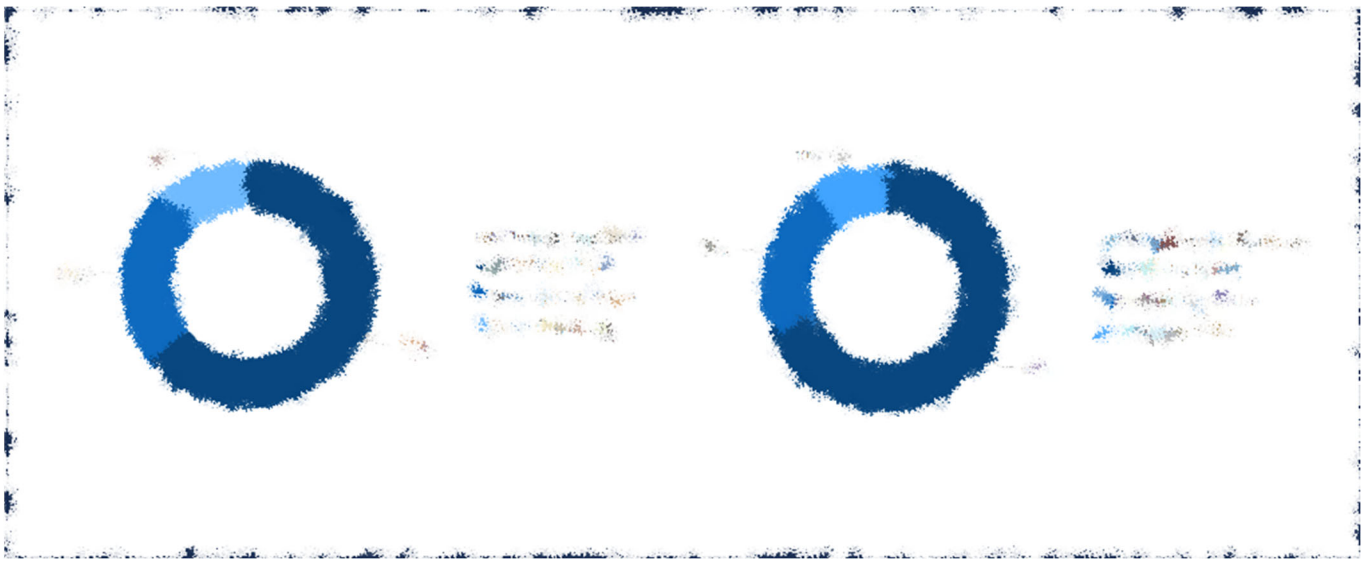


Figure 3.9: IP/Ethernet Surface Area by Organization

Chapter 4: Risk Assessment

Threat Overview

As noted by E-ISAC, CISA, and cyber security professionals, the cyber threat landscape for the electric industry is increasingly complex and challenging. Threats to both information technology (IT) and operational technology (OT) infrastructure have multiplied, evidenced by the persistent compromise of major software components and supply chain vendors[12]. These threats have put electric industry engineers and security professionals under immense pressure to mitigate risks effectively.

E-ISAC plays a critical role in monitoring cyber threats, and it continues to expand system monitoring services through programs like the Cybersecurity Risk Information Sharing Program (CRISP) and other operational technology-focused initiatives. Additionally, E-ISAC has been instrumental in piloting the Department of Energy's Energy Threat Analysis Center, providing better visibility and information sharing of the threat landscape to stakeholders. Certain nation-states continue to persistently target North American critical infrastructure, including the electric grid. In particular, the Office of the Director of National Intelligence reports that China poses a broad, active, and persistent cyber espionage threat to government and private-sector networks, raising concerns about technology-driven authoritarianism[13].

Supply Chain Attacks

A primary concern in recent years has been supply chain risk mitigation. NERC has made it a priority since 2016[14], but the risk continues as nation-state actors and cyber criminals, especially ransomware threat actors, continue to compromise the supply chain. These cyber threat actors exploit third-party vendors' vulnerabilities to gain access to more secure organizations and critical infrastructure. The exploitation of known software vulnerabilities highlights the importance of timely software patching and risk-based vulnerability management programs. The Cybersecurity and Infrastructure Security Agency (CISA) is the operational lead for federal cyber security and the national coordinator for critical infrastructure security and resilience. CISA tracks known exploited vulnerabilities through its known exploited vulnerabilities catalog[15] and the number of known exploited vulnerabilities continues to rise. Credible supply chain threat scenarios include outages of multiple generators, multiple transmission stations, or multiple substations due to the compromise of original equipment manufacturers (OEMs), including but not limited to compromised services, firmware, or unauthorized remote access either interactive or programmatic.

Ransomware

Ransomware remains a persistent threat to the electric industry, with several high-profile attacks causing disruptions to critical operational systems. Additionally, these threats have been identified as having potential use in coordinated attacks, which have emerged as a risk[16], wherein multiple BES Cyber Systems are targeted simultaneously or near simultaneously, leading to adverse reliability impacts on the BPS.

The ongoing grid transformation and increasing penetration of inverter-based resources (IBR) and distributed energy resources (DER) are expanding the attack surface of electrical critical infrastructure[17], necessitating ongoing development and adaptation of cyber and physical security standards and guidelines. NERC initiatives, like Cyber-informed Transmission Planning (CITP)[18] and industry new technology adoption, must be integrated into grid design to strengthen cyber security robustness of the grid.

[12] E-ISAC End of Year Report 2023
[13] Office of the Director of National Intelligence Annual Threat Assessment of the U.S. Intelligence Community
[14] NERC 2022 Annual Report
[15] CISA Known Exploited Vulnerabilities Catalog
[16] Identified in the Low Impact Criteria Review Team (LICRT)
[17] NERC 2023 State of Reliability Technical Assessment
[18] https://www.nerc.com/comm/Documents/NERC_Security_Integration_Strategy_2022.pdf

As the electric industry faces these evolving threats, the efficacy vs. cost of cyber security controls remains a crucial consideration. Implementing measures like INSM can provide a benefit; however budget constraints, staffing limitations, and technological challenges may hinder implementation across the larger number of low impact BES Cyber Systems.

In conclusion, the cyber threat landscape in the electric industry demands vigilant and proactive cyber security measures. The dynamic nature of these cyber threats requires continuous reexamination of minimum cyber and physical security levels to protect critical infrastructure effectively. Security programs cannot rely on a 'check the box' mentality for compliance, but rather focus on implementing security controls beyond the minimum standards. Entities should prioritize supply chain risk mitigation, robust vulnerability management programs with timely software patching, eliminating end of life (EOL) hardware and software, and coordinated incident response to ensure the reliability, resilience, and security of the BPS in the face of evolving cyber threats.

Risk and Impact

To gain a better understanding of the risks and impacts facing the BPS posed by medium impact BES Cyber Systems without ERC and all low impact locations operating without INSM, it is important to understand the changing structure of transmission and generation assets.

Shift from Traditional Generation to Inverter-based Resources

Driven in part by the push towards renewable energy and industry pursuit of decarbonization efforts, the traditional structure of generation continues to change. This change is reflected in the transition from large, centralized generation to smaller, more numerous, and geographically dispersed generation facilities such as wind and solar. To ensure grid reliability and resiliency, it is imperative to continually monitor and reassess BPS risks associated with grid transformation. IBR concerns are well documented by NERC[19] and there is recognition that large-scale grid disturbances involving failures in inverter-based resources, if not addressed, could lead to catastrophic events in the future. While these concerns were focused on operational failures, a cyber security event could also lead to similar impacts and outcomes.

The increasingly dispersed structure of generation has led to, or necessitated, the adoption of innovative technologies as well as the implementation of interconnected networks and remote connectivity to manage these assets effectively. While managing cyber risk at single larger generation facilities is easier to do locally, the management of numerous IBR assets is changing the attack surface of OT grid systems alongside this drastic shift in grid architecture and resource makeup.

Considering these new trends, the historic risk assessment approach of looking at each asset separately may not accurately reflect the current environment or account for emerging risks facing the BPS. Moving forward, simply looking at the independent risk profile of assets containing low impact BES Cyber Systems without consideration for their interconnectivity may not be effective in identifying the residual risk and potential impacts facing the BPS.

Third-party/Vendor Remote Access

Alongside the increased interconnectivity of electric OT systems, another risk factor to low impact BES Cyber Systems is the utilization of third parties to support multiple low impact BES Cyber System operations. Third party vendors often have remote access into these environments to ensure they can effectively offer services to support maintenance and operations. The potential supply chain risk these vendors introduce to the BPS through remote

[19] Quick Reference Guide: Inverter-Based Resource Activities

access represents a credible threat vector. Future NERC Critical Infrastructure Protection (CIP) standards[20] changes are aimed, in part, to further mitigate risks associated with third-party remote access. The 2019 NERC Supply Chain Risk Assessment[21] report, provided an analysis of third-party electronic access to generation facilities and identified that more than 50% of all generation resource locations allow third-party electronic access. The report also noted that with low impact transmission stations and substations, the combined effect of a coordinated cyberattack could negatively impact BPS reliability. The use of vendors or any third parties to support multiple assets containing low impact BES Cyber Systems remotely and the level of connectivity introduced to these systems continues to pose a risk to the BPS. While the use of vendors or third parties to support these dispersed assets may be critical to facilitate decarbonization efforts that are supported by the changing resources mix, this reality comes with increased security risks.

Insider Threats

Insider threats constitute a real risk to any computer system or network, including OT networks. As insider threats often use legitimate, authenticated, and authorized access, there is a need for greater reliance on detection of anomalistic behavior within applications and networks to effectively mitigate against them. Insiders constitute a significant risk for which INSM offers effective tools to aid in detection. Additionally, there are malicious and non-malicious insider threats. Malicious threats are those posed by disgruntled employees. Motivations can vary, they can be motivated by financial gains for example, and particularly those employees with administrative rights to the network pose the greatest risk. Adherence to basic cyber security principles beyond segregation of duties, the concept of least privilege, and network segmentation are less effective against these types of insider threats. Even non-malicious insider threats represent risk to computer networks, particularly OT networks with inherently less security controls implemented. These threats come in the form of poor training, not taking training seriously, or a lack of understanding of the need for a particular security control or another. Poorly trained employees can allow security breaches through facilitating 'tail gating,' bringing insecure devices (i.e., mobile devices, compromised removable media), or disregarding security protocols and procedures (i.e., installing software from unknown or unverified sources). In either case, these types of threats can lead to cyber incidents or cyber compromises. Earlier detection of, and recovery from these cyber events could be better mitigated through enhanced security controls such as INSM.

Risk of Coordinated Attack

Historically, a singular low impact BES Cyber System outage caused by an isolated cyber event would not constitute an adverse reliability impact to the BPS. This explains the impact rating per the CIP-002 risk assessment method and consequently results in less mandated cyber security controls. However, as identified in the Low Impact Criteria Review Team Report published by NERC in 2022[22], the primary risk presented by cyber intrusion of low impact BES Cyber Systems is not from each individually, but rather from low impact locations utilizing interconnectivity that could be exploited in a "coordinated attack" on multiple low impact assets.

As noted in the data collected for this INSM data request **[REDACTED]**

[REDACTED] The implementation of new security requirements, including the use of INSM to assist in the mitigation of these risks, may be necessary to ensure the reliability and security of the BPS moving forward.

The risk of attack against multiple generation or transmission facilities containing low impact BES Cyber Systems, via exploitation of shared vulnerabilities and lateral movement among facilities across their interconnectivity, presents potential impact or outage in aggregate that could meet or exceed that of an outage of a single facility associated with a medium or high impact BES Cyber System. Broadening our risk assessment methodology to ensure all aspects of risk are considered will facilitate a better understanding of risks facing the BPS and assist in building a

[20] Project 2023-04 Modifications to CIP-003
[21] 2019 Supply Chain Risk Assessment
[22] Low Impact Criteria Review Team (LICRT)

comprehensive picture of the risks and impacts posed by low and medium impact BES Cyber Systems that do not implement sufficient mitigating controls, including INSM. Therefore, it is vital that our industry recognizes the aggregate impact of these resources should a successful cyber-attack happen, and incorporate this reality into the development of policies, procedures, and regulations to mitigate this risk.

[REDACTED] This is especially true considering the threat of coordinated attacks, where commonalities in network configurations, fiber, hardware, and software may translate to potential shared vulnerabilities and opportunities for lateral movement. Small organizations may only have accountability for a few substations, while large organizations generally have accountability for hundreds. Therefore, large organizations represent an attractive target to adversaries given a more uniform predictability in the attack surface and higher confidence in a coordinated attack utilizing a focused set of tactics, techniques, and procedures.

Substation and generation locations that contain medium impact BES Cyber Systems without ERC face the same threats as low impact BES Cyber Systems. However, medium impact BES Cyber Systems without ERC must adhere to additional security requirements that low impact BES Cyber Systems are not required to adhere to, per the NERC CIP Standards. Additionally, the lack of ERC lowers but does not eliminate, the effectiveness of most threats against these networks by merit of making both external intrusion and call-homes difficult to impossible. Given the additional control requirements, and the difficulty of achieving lateral movement without available ERC, coordinated attack risk is further minimized. While implementing INSM for medium impact BES Cyber Systems without ERC would offer additional mitigation against prominent threats, the lack of ERC would potentially limit available INSM solutions, their configurations, and their effectiveness. The additional security requirements for medium impact BES Cyber Systems without ERC include:

- Residing within a defined ESP
- Malicious code prevention for network access points
- Event logging & alerting
- Vulnerability assessments

In the absence of INSM, and lacking these additional controls as alternative mitigation, low impact BES Cyber Systems are at increased risk of successful intrusion and compromise from supply chain threats, malware, ransomware, and insider threats. While the loss of an individual low impact BES Cyber System may not have adverse reliability impacts on the Bulk Electric System, the risk of coordinated attack magnifies the potential for a reliability impact. A successful coordinated attack against multiple low impact BES Cyber Systems, taking offline multiple facilities owned or operated by a single entity, would likely match, or exceed the adverse reliability impacts as though a medium or high impact BES Cyber System was compromised. Furthermore, a coordinated attack that hits multiple entities can be expected to be even more devastating. Additional controls for low impact BES Cyber Systems, to expand mitigation against these threats, should be made a priority.

Chapter 5: Challenges and Solutions

INSM serves as a mature set of cyber security controls to detect and respond to the machine speed, scale, and scope of cyber-attacks. However, understanding the challenges with implementing INSM for medium impact BES Cyber Systems without ERC and all low impact BES Cyber Systems is key to effective guidance or regulation. Particularly due to the sheer numbers of locations, INSM for low impact BES Cyber Systems requires critical considerations prior to implementing enforceable standards changes. The following sections contain the major challenges entities assert are the top obstacles to implementing INSM at medium impact BES Cyber Systems without ERC, and all low impact BES Cyber Systems. Each of these areas are expanded upon, with potential solutions offered towards implementing INSM at a future date.

Equipment Retrofit and Network Redesign

Based on the analysis of the data **[REDACTED]**

In response to this challenge, entities could further prioritize cyber security funding and allocate resources specifically for INSM implementations. Risk assessments can help identify critical areas that require immediate attention, allowing for a phased and cost-effective approach. Requiring specific network features for newly constructed assets (e.g., non-flat networks, zones, traffic analysis points) is a forward-looking solution allowing for a future state of grid assets that would facilitate implementing INSM while easing the burden of equipment retrofitting and network redesigns in the future. Entities should further endeavor to integrate such configurations and controls into the design stage of their engineering lifecycle to avoid the resource costs and operational impact risks from the necessary maintenances caused by retrofit and network redesign.

Compliance Burden

Data request respondents owning low impact BES Cyber Systems are split regarding **[REDACTED]** Other respondent comments convey pessimistic expectations for overly lengthy, complex, or burdensome requirements resulting from their interpretation of INSM as defined in FERC Order No. 887.

A potential solution to these issues is to allow industry to familiarize themselves with INSM implementations through the INSM requirements that will result from the FERC order to implement INSM at all high impact BES Cyber Systems and all medium impact BES Cyber Systems with ERC. Allowing entities time for INSM implementations to be in place at all high impact BES Cyber Systems and medium impact BES Cyber Systems without ERC before INSM requirements at additional assets will provide entities the opportunity to allot appropriate budgets, hire qualified staff, as well as source technological solutions providing INSM features and solve other entity specific challenges identified in the INSM data request. Additionally, entities may utilize INSM like solutions to automate asset inventories at medium

and low impact BES Cyber Systems, thus allowing industry familiarity with such solutions prior to mandatory NERC CIP standards changes requiring such solutions.

Budget and Supply Chain Constraints

Another of the primary challenges identified in the data was implementing INSM from the financial aspect. Respondents who own low impact BES Cyber Systems and respondents who own medium impact BES Cyber Systems without ERC agree that costs associated with INSM (e.g., implementation, maintenance, support) are a challenge. **[REDACTED]**

[REDACTED] While the costs are not prohibitive for some entities, the investment should be considered in the context of existing cyber security controls, while also considering the BPS risk posed by entities of different sizes.

Due to the sheer number of locations containing low impact BES Cyber Systems, estimating timelines for industry wide implementation of INSM should consider the potential for delays due to supply chain bottlenecks. These could come in the way of constraints on managed ethernet switches, proprietary hardware sensors, network taps, or even engineering consulting services. With an increase in industry demand the cost of implementation could be significantly higher (e.g., limited vendor options), which may hinder the ability to deploy necessary tools and resources.

These INSM capabilities, as noted previously, are a mature set of cyber security controls. The ability to cost-effectively implement these capabilities, and to achieve a meaningful return on investment that does not cost more to implement than the security benefits INSM provides is paramount in consideration of any future INSM requirements.

Staffing Limitations

Effective INSM requires skilled personnel to install, configure, operate, and maintain the monitoring systems, analyze the data, and respond to security incidents. Many industries, including the electric industry, are experiencing shortages of qualified staff to perform highly technical work of initial implementation and ongoing operations and maintenance of these systems. It is also of note that respondents' comments **[REDACTED]** Respondents who own low impact BES Cyber Systems and respondents who own medium impact BES Cyber Systems without ERC agree that a shortage of qualified staff is a challenge. **[REDACTED]**

The electric industry should invest in cyber security training and workforce development programs to build an internal pool of skilled professionals. Additionally, entities should seek to proactively align technical roles of facility design such as communication networks by acquiring or leveraging the appropriate trained personnel resources. For example, minimally, consulting with telecommunications or network engineers.

Technological Challenges (May Require ERC)

The electric industry is a complex ecosystem with a wide variety of legacy systems, some of which may not be compatible with modern INSM tools and technologies creating a continued reliance on time consuming manual threat analysis, identification, and mitigation. Based on the analysis of the data, the perceptions of respondents who own low impact BES Cyber Systems and respondents who own medium impact BES Cyber Systems without ERC **[REDACTED]**

Entities should conduct a comprehensive assessment of their existing technology infrastructure to identify compatibility issues and determine which legacy systems need upgrading or replacement to support INSM implementations. These assessments will likely include network redesign considerations as well.

Allowing for the adoption of cloud technology for BES Cyber Systems opens opportunities for more diverse INSM solution options, as well as powerful alternative solutions in the way of Managed Detection and Response (MDR) and Managed Security Service Providers (MSSPs). On 17 December 2020, FERC Order Directing Informational Filing Regarding Virtualization and Cloud Computing Services was issued[23], initiating momentum in this area. In Q3 2023, industry submitted two standards authorization requests (SARs) for cloud technology inclusion into the NERC CIP Standards.

1

Challenges and Potential Solutions Summary

INSM offers an improved security posture and bolsters protections against a wide range of risks, including operational disruptions, financial losses, data breaches, ineffective incident response, and cascading failures. Implementing INSM

[23] FERC Order Directing Informational Filing - Virtualization and Cloud Computing Services

would allow for enhanced threat detection, improved response capabilities, and the overall advancement of the cyber security posture of the power industry. As noted however, implementing INSM within the electric industry is a complex undertaking. Addressing budget constraints, workforce limitations, technological challenges, vendor supply chain issues, additional network interconnectivity, and regulatory compliance will require a concerted effort from industry stakeholders, the ERO Enterprise, and FERC.

As the data request responses show, there are a number of hurdles that need to be overcome to allow industry to successfully implement INSM at medium BES Cyber Systems without ERC, and all low impact BES Cyber Systems. NERC finds that overcoming most, if not all of these challenges, to the degree possible will better enhance industry capabilities and facilitate the adoption of INSM solutions for this much larger set of BES Cyber Systems.

Chapter 6: Risk Mitigation

In lieu of implementing complete INSM solutions, alternative controls may be leveraged to mitigate some of the present residual risk posed to medium impact BES Cyber Systems without ERC and all low impact BES Cyber Systems. Expansion of standard best practice cyber security technical controls (e.g., multi-factor authentication (MFA), host-based malicious code detection, perimeter intrusion detection system (IDS), software defined networking (SDN), comprehensive device and application logging, etc.) coupled with effective monitoring activities to empower detection and response may serve as a viable alternate risk mitigation strategy. In particular, for locations containing low impact BES Cyber Systems, implementing foundational controls that increase the awareness and understanding of the underlying networks (e.g., cyber asset inventories, network documentation, and defined network perimeters, etc.) at these locations could further serve as a crucial preliminary step for industry towards establishing INSM requirements at a future date. In this section, with recommended control inclusions from entity respondents, we evaluate several controls for their potential towards alternative risk mitigation in place of INSM. This discussion is not exhaustive, and it is necessary to consider diverse environments, architectures, use-cases, constraints, or other special attributes for the implementation of any such controls.

Ongoing Project 2023-03 Standard Drafting Team (SDT) work amending the NERC CIP standards have highlighted the following two important items to note in the analysis in this study:

- Serial communications are not in scope for INSM requirements with respect to high and medium impact BES Cyber Systems
- The FERC Order 887 directing NERC CIP changes and the commission of this study was not intended to mandate that ERC must be implemented to facilitate implementations of INSM[24]

Additionally, INSM implementations include several facets and capabilities outlined in the FERC Order 887, including:

- Baselining of network traffic25
- Detect unauthorized activity, connections, devices, and software.
- Logging network traffic
- Maintaining logs and other data collected regarding network traffic.
- Implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures.

Alternate Mitigating Controls

Alternate mitigating controls worthy of evaluation for alternative risk mitigation to INSM include controls that are not currently present within the NERC CIP-003 standard, which sets the security baseline for assets containing low impact BES Cyber Systems. **[REDACTED]**

[24] Project 2023-03 Standard Drafting Team (SDT) work is on-going. Final results of this project and any subsequent standards changes may vary from the time of the filing of this INSM study report with FERC.

[25] Baselining, and the specific requirements that define it, will be finalized at the conclusion of the SDT work. In this context, baselining is referring to understanding what 'normal' network traffic looks like within a trust zone.

Multi-factor Authentication

MFA is a technology that reduces the risk of compromised credentials being used for unauthorized remote access. Such technologies ensure authentication systems within BPS environments are robust and effective. In an OT system, such as those in our industry, a defense-in-depth strategy includes MFA for remote access.[26] MFA has become a necessary cyber security control for remote access that should be considered to bolster the collective security posture of the electric grid and manage the growing risk associated with IBR trends. Independent of INSM, NERC sees MFA as a crucial control to mitigate against numerous threats potentially initiated through compromise of remote access capabilities.

Given the diversity of solution offerings, the multitude of best practice implementations for interactive remote access, and the widespread cross-industry precedent for MFA today, this control is ripe for application to all BES Cyber Systems with remote access, including lows. Additionally, the common constraints of low impact BES Cyber Systems and their cyber assets do not preclude most MFA implementations. Related to authentication, the following SDT project work should also be noted:
[REDACTED]

Perimeter-Based Malicious Code Detection

[REDACTED] The boundaries between the secured internal BES Cyber System network and outside networks (e.g., Enterprise IT, the internet, or other BES Cyber Systems) provide opportunities to implement a network intrusion detection system (NIDS), often standalone or as part of a firewall. Like solutions that achieve INSM, these enable traffic inspection which can reduce risks by detecting suspicious behavior as well as malicious binaries in transit.

While perimeter-based NIDS has been seen as an effective bastion defense for years, high risk threats including supply chain attacks and insider threats may utilize authorized traffic for lateral movement between networks, potentially passing checks by network traffic inspection detection capabilities of a perimeter-based NIDS as well as any network access control lists such as firewall policies. However, dependent on network design, a key benefit of perimeter-based NIDS is in the potential coverage of traffic between multiple BES Cyber Systems with a single deployment, **[REDACTED]** This benefit allows a perimeter-based NIDS to potentially achieve highly cost-effective risk mitigation. Therefore, NERC finds perimeter-based IDS is a potentially viable alternative control, albeit a less effective mitigation versus the more comprehensive detection within each internal network as delivered by INSM.

Survey respondents provided estimations on current implementation of perimeter-based malicious code detection across their footprint. Analysis shows that **[REDACTED]**

[REDACTED]

[REDACTED]
[REDACTED]

Host-Based Malicious Code Detection

The introduction of malicious code can be mitigated through detection or prevention at the network level, as previously discussed, or at the host level. Host-based malicious code detection may include anti-virus, anti-malware, or more modern solutions such as endpoint detection and response (EDR). Periodic and real-time host-based scans of cyber assets, especially servers, HMIs, or other systems that meet the necessary operating system and hardware requirement for such controls, have viability even in electric OT networks, even if not ubiquitously.

Just as with the other controls not currently required for low impact BES Cyber Systems, malicious code detection is a critical component of cyber security defense-in-depth strategies **[REDACTED]**

[26] NIST Special Publication NIST SP 800-82r3

Software Defined Networking

Software defined networking (SDN) reduces risk through the intelligent restriction of network traffic routes, automated routing failovers in the event of communication path failures, enabling network segregation, and provides greater general control and awareness of the network **[REDACTED]** SDN provides preventative controls restricting endpoint communications to those defined specifically by the network administrator. These rules prevent attackers who may have breached the network from moving laterally without any restrictions. Additionally, some SDN implementations also provide detection controls by issuing alerts on identified anomalous traffic that does not meet the predefined SDN rule sets. Lastly, responses to active cyber incidents such as containment efforts are also facilitated through the logging capability of SDN controllers.

Future requirements through new or revised standards may be utilized for enhancing the overall industry security footprint through requirements aimed at newly designed and built grid assets (e.g., substation design based on frameworks like IEC 62443).

Foundational Controls

Exploring alternative mitigation strategies in the way of foundational controls that could be more easily implemented utilizing existing workforces, budgets, and accounting for the myriad constraints outlined in this study would provide necessary added layers of protection against cyber threats and the risks they pose through enhancing defense-in-depth strategies. **[REDACTED]**

[REDACTED]

Asset Inventory

In the spirit of knowing first what you have, and therefore what must be protected, asset inventories are a critical foundational component of any cyber security framework. Placing advanced cyber security controls ahead of foundational components may not be prudent or may be infeasible in many cases. Performing maintenance, including highly impactful network redesigns or retrofits can be disastrous without thorough understanding of what underlying cyber assets will be impacted. For both security and business continuity, understanding the criticality of those assets is necessary to effectively assess risk and develop effective and reasonable risk mitigation strategies. Without proper knowledge of the assets in a network, as well as knowledge of the network itself, implementation of a solution such as INSM could easily be sub-optimal to dysfunctional. **[REDACTED]**

Defensible Network Architectures

[REDACTED]

[REDACTED]

Electronic Security Perimeters

In the same vein as asset inventories and knowing what you have as a prerequisite to protecting it, establishing some form of a network trust zone, with defined network boundaries, including documentation of that network and its boundaries, must necessarily come before the development of strategies to protect that network and ultimately the cyber assets contained therein. This is not a new paradigm under NERC CIP, though its language and definitions have evolved over time, and are under further review in ongoing standards work.

On-going SDT work for high and medium impact BES Cyber System INSM requirements highlight the inherent difficulty in defining definitions (e.g., 'baselines,' 'anomalous activity,' 'high degree of confidence,' etc.), control capabilities, how they are implemented, and where the requirements start and stop from a network perspective. All

of which point to the minimum requirement to define CIP-networked environments, and in particular network boundaries. **[REDACTED]**

[REDACTED]

[REDACTED]

Logging and Alerting

Security monitoring depends entirely upon the delivery of vital information related to suspicious activity being delivered to the eyes and ears of those responsible for monitoring. This demands the configuration of the numerous critical logging and alerting features amidst both operational systems and tools, as well as security applications.

Logging and alerting responsible parties when physical security alarms are received, or logging of pre-defined categories such as those currently in CIP-005 are foundational components of a strong security posture. Further, these controls enable detection and effective cyber incident response.

[REDACTED]

Technology Lifecycle Refresh

Requiring end of life (EOL) assets to be upgraded to equipment that can be supported by manufacturers and application developers **[REDACTED]**

Low Impact BES Cyber System Information

[REDACTED]

NERC CIP Standards Projects

As noted, on-going NERC Standards development for CIP-003 is underway. Project 2016-02 drafting of CIP-003 modifications includes requirements for monitoring, disabling, and implementing malicious code detection around vendor remote access. Project 2023-04 aims to increase the security baseline of low impact BES Cyber Systems in a multitude of areas and will include a subset of the controls evaluated above which may serve as alternative mitigation to INSM. Among these include, requiring a form of authentication for remote access, and some form of malicious code detection requirements. The new standard version, should it pass, will require entities to meet requirements for malicious code detection for inbound and outbound communications, authentication of remote access users, including vendors, and information protection measures of user authentication information while in transit.

Chapter 7: Conclusion

The cyber threat landscape for the electric industry is increasingly complex and challenging. Threats to both IT and OT infrastructure continue to grow, as evidenced by the persistent compromise of major software components and supply chain vendors along with the growing number of known vulnerabilities. Cases of network compromises and attacker persistence abound, with the 2020 SolarWinds attack[27] being a prime example. The threat of attackers compromising networks and going undetected within a trust zone constitutes a risk to the BPS as noted in the FERC order directing NERC to perform this study. Ongoing grid transformation, **[REDACTED]** These threats have put the electric industry's security professionals and regulators under immense pressure to mitigate risks effectively.

[REDACTED]
The evaluation of alternative controls to mitigate the risk of coordinated cyber-attacks from threats such as supply chain attacks and insider threats, leads to a couple of conclusions. **[REDACTED]** NERC recognizes INSM as the current most effective solution in providing broad coverage in both areas, and most crucially, offering effective mitigation against present and emerging cyber risk which is expected to grow amidst the increasing proliferation of IBRs and continued IT-OT network convergence.

When combined with foundational cyber security controls, INSM is an effective detective control, alerting security professionals to potential attacks and facilitating quicker incident response, mitigation of adverse impacts, and aiding in recovery and investigative efforts. **[REDACTED]** Threat scenarios involving non-routable networks are less likely and currently available INSM solutions are designed to function within predominantly IP-based/ethernet networks.

Standards changes requiring the implementation of INSM for low impact BES Cyber Systems prematurely, which fail to give industry enough time to plan for and develop the necessary prerequisites to implement INSM, nor give entities time to address budget and resource planning for such significant system changes, may result in less effective implementations, poor compliance, and may inadvertently incentivize entities to avoid modernizing their infrastructure.

INSM is a mature set of controls, predominately entailing monitoring of east-west traffic in a trusted network zone(s). However, INSM implementation does bring challenges associated to the existing network architectures being retrofit to accommodate INSM solutions, **[REDACTED]** With unlimited resources (e.g., time, people, money) there would be no need for analysis on whether to implement INSM at medium impact BES Cyber Systems without ERC and low impact BES Cyber Systems. However, given the constraints on these resources that we must contend with, NERC recommends a phased approach in the coming years.

Roadmap

To prevent INSM being a less effective bolted-on cyber security control, NERC asserts that there needs to be a solid foundation to build INSM capabilities into grid defenses at medium impact BES Cyber Systems without ERC, and all low impact BES Cyber Systems. To facilitate INSM requirements at low impact BES Cyber Systems and medium impact BES Cyber Systems without ERC, NERC recommends industry, through the Reliability and Security Technical Committee (RSTC), develop a roadmap that improves comprehensive cyber security controls required for the additional grid assets as outlined in the order. The roadmap would include a phased approach to raising the bar of existing cyber security controls required under the current NERC CIP-003 Standard. These changes would include filling what NERC asserts are foundational and necessary pre-requisites to implementing a defensible architecture that includes INSM resulting in the largest improvements to reliability and meaningful return on investment, while simultaneously not overburdening industry in the interim. Such a roadmap would allow industry the necessary time and the ability to address the challenges of implementing INSM for the larger set of grid assets under consideration.

[27] CISA Alert-Active Exploitation of SolarWinds Software

The high-level roadmap would include NERC CIP standards changes such as:

- Requirements for low impact BES Cyber System asset inventories
- Requirements for designing, constructing, and documenting defensible network architectures to remove insecure by design network configurations (i.e., segmentation, conduits & zones, traffic analysis points, etc.)
- Requirements for strong multi-factor authentication for interactive remote access
- Standards changes should not negatively incentivize entities to delay changes, or implement BES Cyber Systems in order to circumvent standards requirements through compliance loopholes or abuse of exceptions such as:
    - Maintaining non-supported end of life equipment and applications to alleviate compliance overhead to the detriment of security.

Other components may also exist that would need to be codified for such a roadmap. As noted in this report, on-going work by an existing NERC Standards Drafting Team will require additional security controls that will serve to reduce the risk of remote attackers gaining access to protected BES Cyber Systems. These impending NERC CIP changes, and the subsequent industry adoption and implementation of INSM technologies at high and medium impact BES Cyber Systems, will serve to ready industry to overcome challenges outlined in this report including potential supply chain bottlenecks associated with the entire industry attempting to source products and services simultaneously. Additionally, the necessary budgeting preparations, staffing requirements, and other challenges outlined herein will benefit from the lead time between INSM requirements being enforceable at high impact and medium impact with ERC BES Cyber Systems and future requirements for INSM at the much larger set of medium without ERC and all low impact BES Cyber Systems. Additional features of the proposed roadmap for future INSM requirements should also consider risk as it pertains to entities with much smaller footprints and not overly burden those entities with lower asset counts, and therefore, lower BPS risk.

Monitor Risk

NERC advises the Commission to allow INSM implementations to proceed at high impact BES Cyber Systems and medium impact BES Cyber Systems with ERC, while NERC, the E-ISAC, and FERC continue to monitor BPS risk to inform any necessary adjustments to an INSM roadmap timeline for low impact BES Cyber Systems and medium impact BES Cyber Systems without ERC.

Appendix A: Data Request Questions

Below are the questions provided to entities for Section 1600 Data Request. Entities were required to submit answers to these questions for each of the registered NERC Compliance Registry (NCR) numbers assigned to an entity.

1. (Required Response) Provide the number of (a) substation and (b) generation locations containing medium impact BES Cyber Systems **with** ERC[28]. (Comment field can be used to provide explanation for responses if needed.)
2. (Required Response) Provide the number of (a) substation and (b) generation locations containing medium impact BES Cyber Systems **without** ERC. (Comment field can be used to provide explanation for responses if needed.)
3. (Required Response) Provide the number of (a) substation, (b) generation, and (c) Control Center locations containing low impact BES Cyber Systems **with** ERC. (Comment field can be used to provide explanation for responses if needed.)
4. (Required Response) Provide the number of (a) substation, (b) generation, and (c) Control Center locations containing low impact BES Cyber Systems **without** ERC. (Comment field can be used to provide explanation for responses if needed.)
5. (Required Response) Provide the estimated percentages, totaling 100% of network configurations for your low impact BES Cyber Systems.
    a. Completely IP-based
    b. Majority IP-based with minimal serial (or other non-IP connectivity)
    c. Completely serial (or other non-IP connectivity)
    d. Majority serial (or other non-IP connectivity) with minimal IP-based connectivity
    e. Approximately 50/50 mix of IP-based and serial (or other non-IP connectivity) present at location
6. (Required Response) Provide the estimated percentages, totaling 100% of network configurations for your medium impact BES Cyber Systems **without** ERC.
    a. Completely IP-based
    b. Majority IP-based with minimal serial (or other non-IP connectivity)
    c. Completely serial (or other non-IP connectivity)
    d. Majority serial (or other non-IP connectivity) with minimal IP-based connectivity
    e. Approximately 50/50 mix of IP-based and serial (or other non-IP connectivity) present at location
7. (Required Response) From (1) least challenging to (5) most challenging, independently rate each of the listed potential technological, logistical, or other challenges involved in extending INSM to additional medium impact BES Cyber Systems (e.g., medium impact without ERC) and low impact BES Cyber Systems (e.g., all low impact):
    a. (Required Response) Implementation of INSM may require equipment retrofit and network redesign.
    b. (Required Response) Compliance burden associated with implementing INSM (e.g., lack of a discrete list of low impact BES Cyber Systems and defined low impact electronic security perimeters).
    c. (Required Response) The overall costs associated with INSM (e.g., implementation, maintenance, support).

[28] As it pertains to low impact BES Cyber Systems, ERC is being used in the context of this data request to refer to external connectivity to/from the BES Cyber System although the defined term is not used in association with low impact BES Cyber Systems within the NERC CIP standards.

d. (Required Response) Technical supply chain constraints (e.g., hardware/software availability).

e. (Required Response) Shortages of qualified staff (e.g., implementation, maintenance, support).

f. (Required Response) INSM implementation may require expanding ERC at some BES Cyber System locations, thereby increasing the attack surface.

g. (Optional Response) Other challenges.

8. (Required Response) Provide the estimated percentage of low impact BES Cyber Systems that currently have network based malicious code detection. Malicious code detection can be accomplished either internally on the BES Cyber System network or at the BES Cyber System network boundary.

9. (Optional Response) List recommended alternative solutions or controls to mitigate the risk posed[29] to BES Cyber Systems operating without INSM. **Please keep answers as concise as possible**.

10. (Optional Response) For existing implementations of INSM at current BES Cyber System locations, what solutions (e.g., vendors, products, and service providers) are deployed? **Please provide a concise high-level list**.

[29] See FERC Docket No. RM22-3-000; Order No. 887 Section 15

Appendix B: List of Contributors and Acknowledgments

The following individuals participated in the development of the 1600 INSM data request and the completion of this study. This group included a team of ERO Enterprise experts working collaboratively to complete the data request, perform the analysis of the data, and development to this final report as directed by FERC order 887. We thank them for their contributions to the security and reliability of the BPS.

Name	Company
Carl Epping	Midwest Reliability Organization
Dan Goodlett	North American Electric Reliability Corporation
Larry Collier	North American Electric Reliability Corporation
Marisa Hecht	North American Electric Reliability Corporation
Michaelson Buchanan	North American Electric Reliability Corporation
Jeremy Withers	Reliability First
Lindsey Mannion	Reliability First
Jermaine Green	SERC Reliability Corporation
Steven Keller	SERC Reliability Corporation
Devin Kitchens	Texas Reliability Entity, Inc.
Morgan King	Western Electricity Coordinating Council
Tiffany King	Western Electricity Coordinating Council

Public