UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE ISO/RTO COUNCIL

The ISO/RTO Council ("IRC")[1] submits these comments in reply to the Notice of Proposed Rulemaking ("NOPR") that the Federal Energy Regulatory Commission ("FERC" or "Commission") issued in Docket No. RM22-3-000 on January 20, 2022.[2] In the NOPR, the Commission proposes to direct the North American Electric Reliability Corporation ("NERC") to develop and submit for Commission approval new or modified Reliability Standards that require internal network security monitoring ("INSM") within a trusted Critical Infrastructure Protection ("CIP") networked environment for high and medium impact Bulk Electric System ("BES") Cyber Systems. The IRC supports the Commission's proposal and provides recommendations on how to best retain flexibility in how registered entities would implement the revised or new CIP Reliability Standards.

[1] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"); California Independent System Operator ("CAISO"); Electric Reliability Council of Texas, Inc. ("ERCOT"); the Independent Electricity System Operator of Ontario, Inc. ("IESO"); ISO New England Inc. ("ISO-NE"); Midcontinent Independent System Operator, Inc. ("MISO"); New York Independent System Operator, Inc. ("NYISO"); PJM Interconnection, L.L.C. ("PJM"); and Southwest Power Pool, Inc. ("SPP"). The AESO and IESO are not FERC-jurisdictional, however join these comments.

[2] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems,* Notice of Proposed Rulemaking, 178 FERC ¶ 61,038 (2022).

I. INSM IS A NECESSARY AND VALUABLE SECURITY PRACTICE

Recognizing that INSM is a necessary and valuable security practice, the IRC recommends focusing the security objective of the new or modified CIP Reliability Standards on registered entities' need to develop a holistic internal network monitoring solution to detect and respond to anomalous activity. The NOPR proposes to "direct that NERC, as the [Electric Reliability Organization ("ERO")], develop new or modified CIP Reliability Standards requiring that applicable responsible entities implement INSM for their high and medium impact BES Cyber Systems."[3] Furthermore, the NOPR describes the three security objectives regarding INSM that the new or revised CIP Reliability Standards, should address as follows:

> First, any new or modified CIP Reliability Standards should address the need for each responsible entity to develop a baseline for their network traffic by analyzing expected network traffic and data flows for security purposes. This objective reduces the likelihood that an attacker could exploit legitimate cyber resources to: (1) escalate privileges, i.e., exploit software vulnerability to gain administrator account privileges; (2) move undetected inside a CIP networked environment (i.e., trust zone); and (3) execute unauthorized code, e.g., a virus or ransomware. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP networked environment (i.e., trust zone). This objective reduces detection time, which shortens the time an attacker has to leverage compromised user accounts and traverse over unmonitored network connections. And third, any new or modified CIP Reliability Standards should address the ability to support operations and response by requiring responsible entities to: (1) log and packet capture network traffic; (2) maintain sufficient records to support incident investigation (i.e., monitoring, collecting, and analyzing current and historical evidence); and (3) implement measures to minimize the likelihood of an attacker removing evidence of their Tactics, Techniques, and Procedures (TTPs) from compromised devices. Logging, including packet capture, of network traffic is critical for a responsible entity to assess the severity of the attack, assess the scope of systems compromised, and devise appropriate mitigations.[4]

[3] NOPR at P 31.

[4] *Id*.

The IRC agrees with the need to implement INSM for high and medium BES Cyber Systems. However, the IRC notes that some aspects of the stated security objectives are already addressed under existing CIP Reliability Standards, *e.g.* CIP-007-6 (Cyber Security – Systems Security Management), which requires event logging (and alarming upon failure) and methods to deter, detect or prevent malicious code on high and medium impact BES Cyber Systems, as well as CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments), which requires the authorization and documentation of any changes to existing baseline configurations of high and medium impact BES Cyber Systems. Additionally, the IRC recommends that the security objectives and any new or modified CIP Reliability Standards align with *NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations.*[5] Chapter 3.19 of that NIST Special Publication contains System and Information Integrity Controls that pertain to the security objectives in the NOPR. For example, under "System Monitoring," there is a control for Unauthorized Network Services and a control to Optimize Network Traffic Analysis.

II. FLEXIBLE, OBJECTIVE-BASED, AND RISK-BASED CIP RELIABILITY STANDARDS ALLOW REGISTERED ENITIES TO SELECT AN APPROPRIATE SOLUTION FOR THEIR ENVIRONMENTS

On December 7, 2021, FERC approved Reliability Standards CIP-004-7 (Cyber Security – Personnel & Training) and CIP-011-3 (Cyber Security – Information Protection).[6] The IRC is pleased with this progress as these standards will enhance BES reliability as they create increased choice, greater flexibility, higher availability and reduced cost options for entities to

[5] Joint Task Force Transformation Initiative Interagency Working Group (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[6] *Letter Order Approving the Petition of the North American Electric Reliability Corporation for the Approval of Reliability Standards CIP-004-7 and CIP-011-3*, Docket No. RD21-6-000 (2021).

manage their BES Cyber System Information by providing a secure path towards utilization of modern third-party data storage and analysis systems, also known as cloud service providers. Further revisions to the CIP Reliability Standards will be needed to allow for flexibility in determining which solutions are appropriate to implement a holistic security monitoring approach.

The IRC recommends that any new or modified CIP Reliability Standards allow registered entities to select the appropriate INSM solution for their environment. Although registered entities with small CIP environments could (and may prefer to) conduct network traffic analysis as envisioned under the NOPR, this method can be administratively burdensome for registered entities with large CIP environments, such as ISOs/RTOs. The reason for this is that network solutions, such as micro-segmentation, require an entity to capture every network packet for all flows within the network and then redirect this traffic to a security analyzer to be sifted for exceptions or anomalies. While this method provides full visibility into all flows that reside in the network, it is more manageable in small environments where the quantity of data to be analyzed is practicable and lends itself to this type of review. In large CIP environments, however, it is significantly more difficult for registered entities to capture all lateral movement between hosts and then analyze the large quantity of data captured to identify and mitigate security risks. In addition, capturing all lateral movement between hosts is likely to generate a large volume of false positive anomalous activity instances that an entity would need to analyze, potentially obscuring true positive anomalous behavior.

Consequently, large CIP environments may perform better with a system solution where tools are able to pattern match and log changes via machine learning. System solutions for anomaly detection, such as monitoring of east-west network traffic (also known as inter-VLAN

traffic monitoring), offer registered entities with large CIP environments a more efficient way to summarize data and identify anomalies than a network solution that utilizes open capture, as system solutions *only log exceptions or changes* as opposed to logging *all* activity. It would be significantly more advantageous for registered entities with large CIP environments to analyze these anomalies in this manner.

The IRC supports the ability for registered entities to be able to adopt best practices in anomaly detection and response. Therefore, new or revised CIP Reliability Standards should be objective-based. Objective-based CIP Reliability Standards focus on *achieving* defined security objectives rather than *how* security objectives are met. As mentioned above, many registered entities are already performing some type of INSM under existing CIP Reliability Standards. Objective-based Reliability Standards would allow registered entities to use or expand the use of existing tools to meet security objectives. For example, Zero-Trust elements could take the form of both system-based and network-based solutions. Therefore, a framework that permits a variety of solutions provides registered entities with the ability to select a suitable solution to meet the intent of the NOPR. An implementation of Zero-Trust Architecture within an entity's defined Electronic Security Perimeter would meet or exceed all the objectives outlined within the NOPR. Such an implementation should be a permissible choice but not one specifically required by CIP Reliability Standards.

Another benefit of objective-based Reliability Standards is that they would allow registered entities to keep pace with emerging technology solutions. Under objective-based standards, registered entities would be authorized to timely migrate to emerging INSM solutions that best meet their needs, provided security objectives continue to be met. The Reliability Standards development process can take several years. For example, Project 2016-02 Modifications to CIP

Standards has been in development process for six years. Objective-based Reliability Standards minimize the need to revise Reliability Standards as long as the objectives remain constant.

Risk-based Reliability Standards will also ensure that compliance and security objectives are aligned. Security should not take second place to compliance whereby registered entities feel compelled to implement more than one INSM solution to meet both compliance and security objectives. The IRC recommends that any new or modified CIP Reliability Standards require registered entities to develop an INSM plan that states security objectives. Moreover, any such Reliability Standards should require registered entities to both validate implementation of the INSM plan and provide evidence/reports on the achievement of the plan's security objectives.

Given the importance of INSM, the IRC anticipates a Standards Drafting Team would need one to two years to develop new or modified CIP Reliability Standards to meet this proposed directive and would defer to the Standards Development Team on establishing an implementation date.

III. RECOMMENDATION FOR TECHNICAL WORKSHOP TO DISCUSS TECHNICAL CAPABILITIES

The IRC recommends that the Commission hold a technical workshop to facilitate informal discussion regarding the required technical capabilities of a network behavior or network traffic analysis or system, and the possible technical solutions available to meet the INSM security objectives. Many of the newer security monitoring tools from quality vendors are cloud-based and existing CIP Reliability Standards do not currently allow for the utilization of these tools. The industry, the ERO, and the Commission would benefit from further discussion on this topic.

IV. CONCLUSION

The IRC respectfully requests that the Commission accept and consider these comments.

/s/ Diana Wilson
Diana Wilson
Director Enterprise Risk Management and Compliance
Alberta Electric System Operator
#2500, 330 — 5 Avenue SW
Calgary, Alberta T2P 0L4
Diana.wilson@aeso.ca

/s/ Devon Huber
Devon Huber
Senior Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street
West Toronto, Ontario M5H1T1 Canada
devon.huber@ieso.ca

/s/ Raymond Stalter
Robert E. Fernandez
General Counsel
Raymond Stalter
Director of Regulatory Affairs
Chris Sharp
Senior Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, NY 12144
gcampbell@nyiso.com

/s/ Thomas DeVita
Craig Glazer
Vice President-Federal Government Policy
Thomas DeVita
Senior Counsel
PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, Pennsylvania 19403
thomas.devita@pjm.com

/s/ Andrew Ulmer
Roger E. Collanton
General Counsel
Anthony Ivancovich
Deputy General Counsel, Regulatory
Andrew Ulmer
Assistant General Counsel
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
aulmer@caiso.com

/s/ Margo Caley
Maria Gulluni
Vice President & General Counsel
Margo Caley
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

/s/ Kristina Tridico
Kristina Tridico
Deputy General Counsel
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, IN 46032
ktridico@misoenergy.org

/s/ Paul Suskie
Paul Suskie
Executive Vice President & General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

/s/ Chad V. Seely
Chad V. Seely
Vice President & General Counsel
Nathan Bigbee
Assistant General Counsel
Electric Reliability Council of Texas, Inc.
8000 Metropolis Drive,
Building E, Suite 100
chad.seely@ercot.com

CERTIFICATE OF SERVICE

I hereby certify that I have this day e-served a copy of this document upon all parties listed on the official service list compiled by the Secretary in the above-captioned proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated this 28th day of March, 2022 in Carmel, Indiana.

/s/ Julie Bunn

Julie Bunn
Midcontinent Independent
System Operator, Inc.
720 City Center Drive
Carmel, IN 46032
317-249-5400