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**

JOINT COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION AND THE REGIONAL ENTITIES IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") and the six Regional Entities,[1] collectively the "Electric Reliability Organization ("ERO") Enterprise," submit comments on the Federal Energy Regulatory Commission ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR") proposing to direct Critical Infrastructure Protection ("CIP") Reliability Standards development addressing internal network security monitoring for high and medium impact Bulk Electric System ("BES") Cyber Systems.[2] In addition, the Commission seeks comment on whether it would be useful or practical to implement internal network security monitoring for networks including low impact BES Cyber Systems and whether a subset of low impact BES Cyber Systems would be appropriate for applicability.

The ERO Enterprise supports the Commission's continued focus on strengthening the cyber security posture of Responsible Entities[3] to enhance reliability and security. Furthermore, the ERO Enterprise recognizes the importance in leveraging the correct method to address threats that evolve quickly. As such, while the ERO Enterprise draws from a variety of methods to address cyber security (e.g., information sharing, guidelines, alerts, etc.), the ERO Enterprise supports

[1] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.

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

[3] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

considering standards development to address the risks outlined in the NOPR. To that end, the ERO Enterprise looks forward to stakeholder comments on the NOPR regarding the appropriateness of internal network security monitoring in Reliability Standards requirements or whether there are other options or methods to address the risks outlined in the NOPR. The ERO Enterprise provides comments on specific aspects of the Commission's proposal and respectfully requests that the Commission consider these comments in future issuances in this proceeding.

I. COMMENTS

As noted above, the Commission's NOPR proposes to direct NERC to develop requirements within the CIP Reliability Standards for internal network security monitoring of high and medium impact BES Cyber Systems. The Commission noted that bad actors might leverage vendors or others with authorized access to a network to attack these systems.[4] As noted in the NOPR, an Executive Order[5] instructed federal agencies to move towards more zero trust principles,[6] and the Commission stated that internal network security monitoring is a "fundamental element of the zero trust approach."[7] The Commission further noted that perimeter-based security controls, such as the Electronic Security Perimeter ("ESP"),[8] are not designed to detect suspicious

---

4 NOPR at P 17.

5 Executive Order No. 14,028, 86 Fed. Reg. 26633 (May 12, 2021), https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

6 NOPR at P 22. The NOPR at P 22, fn 35 defines zero trust as follows: "Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). *See generally National Institute of Standards and Technology* (NIST), NIST Special Publication 800-207 Zero Trust Architecture, (Aug. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (providing a general definition of zero trust and general information and cases where zero trust may improve an entity's overall cybersecurity posture)."

7 *Id.* at P 30.

8 The NERC Glossary defines an ESP as "the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." NERC, *Glossary of Terms Used in NERC Reliability Standards* (June 28, 2021), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

activity within the network.[9] As a result, the Commission stated that internal network security monitoring could detect this sort of activity.[10] In addition, the NOPR requests comment on whether it would be useful or practical to implement internal network security monitoring for networks including low impact BES Cyber Systems and whether a subset of low impact BES Cyber Systems would be appropriate for applicability.[11]

The ERO Enterprise supports efforts to address the risks identified in the NOPR and agrees that internal network security monitoring would be an appropriate approach to address these risks. Should the Commission determine to adopt its proposal in a final rule in this proceeding, the ERO Enterprise requests the Commission defer to NERC regarding the appropriate timeline for standards development, so the issues identified below, and in other comments received in response to the NOPR, can receive the proper consideration in the standards development process. Moreover, regarding low impact BES Cyber Systems, the ERO Enterprise notes that requirements for internal network security monitoring could encounter several challenges during development and that any subset considered should take routable connectivity into account, further demonstrating the need for deference to the NERC standards development process.

A. The ERO Enterprise supports addressing the risks outlined in the NOPR and agrees that the proposed internal network security monitoring approach is appropriate.

In the NOPR, the Commission identifies certain risks to BES Cyber Systems that may exist under the current CIP Reliability Standards structure. These risks include insider threats or supply chain attacks. For instance, the Commission cited the SolarWinds event in 2020 as the type of

9 NOPR at P 17.
10 *Id*. at P 26.
11 *Id*. at P 33-4.

activity internal network security monitoring could detect.[12] Similarly, the ERO Enterprise has recognized and addressed supply chain threats as evidenced by its focus on supply chain activities.[13] In fact, NERC worked with FERC staff on supply chain vendor identification to assist entities in noninvasive identification of the network interface controller.[14] This identification, similar to internal network security monitoring, permits entities to better understand components or activities on their systems. As such, the ERO Enterprise appreciates the risks identified in the NOPR and agrees that proposed internal network security monitoring is an appropriate approach to address these risks.

Internal network security monitoring is a technical method to maximize early detection of cyber security vulnerabilities and incidents on networks. This control supports the capability of leveraging emerging technologies such as machine learning or artificial intelligence, pattern analysis, and negative space detection. It may provide the capability of aggregating information from existing controls in detecting physical and cyber anomalies. For high and medium impact BES Cyber Systems, internal network security monitoring would include monitoring activity within the ESP. The ESP architecture controls inbound and outbound access to high and medium BES Cyber Systems, and Reliability Standard CIP-005-6, Requirement R1, Part 1.5 requires malicious communications monitoring at the Electronic Access Point on the ESP, not necessarily monitoring of activity of those who already have access to the network. Furthermore, given the flexibility of determining how a BES Cyber System could be grouped and depending on the

---

[12] NOPR at P 18.

[13] As one example, see the ERO Enterprise comments filed in response to the Notice of Inquiry regarding potential risks to the BES posed by equipment and services produced by certain entities. *Joint Comments of the North American Electric Reliability Corporation and the Regional Entities in Response to Notice of Inquiry*, Docket No. RM20-19-000 (Nov. 23, 2020).

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

methods used to meet certain CIP requirements, there are times where there is not east-west, internal ESP, monitoring. Therefore, internal network security monitoring amongst the BES Cyber Assets in a BES Cyber System is an appropriate way to address the risk posed by bad actors leveraging trusted individuals or methods to gain access to a network. The ERO Enterprise considers internal network security monitoring an appropriate approach to do so.

Current CIP Reliability Standards provide some flexibility in how Responsible Entities identify, categorize, and monitor applicable BES Cyber Systems, including the option to implement internal network security monitoring to meet certain requirements even though it is not specifically required. Responsible Entities may categorize one BES Cyber Asset or a group of BES Cyber Assets in varying configurations to constitute a BES Cyber System under Reliability Standard CIP-002-5.1a. For instance, one Responsible Entity with a Control Center may consider all BES Cyber Assets at that Control Center as one BES Cyber System or just the BES Cyber Assets associated with the Energy Management System as a BES Cyber System. Moreover, there is flexibility in monitoring network connectivity to and from these systems under the CIP Reliability Standards. While certain communications to applicable systems must be controlled through an Electronic Access Point on the ESP, Responsible Entities could use internal network security monitoring as a method to further detect malicious code for applicable systems within the ESP under CIP-007-6, Requirement R3, Part 3.1 or for detecting malicious communications pursuant to CIP-005-6, Requirement R1, Part 1.5. These requirements, however, could be met through other methods. Given this flexibility in grouping of devices and monitoring of network traffic, the CIP Reliability Standards could benefit from consideration of internal network security monitoring requirements as a consistent means of gaining visibility and awareness within an ESP.

The ERO Enterprise also recognizes the importance of maturing security controls pertaining to zero trust principles within Reliability Standards. Through the Project 2016-02 Modifications to CIP Standards development effort, the ERO Enterprise and industry stakeholders have demonstrated support for incorporating zero trust principles into the CIP Reliability Standards as the project addresses methods to permit more use of the security benefits for virtualized technologies. The ERO Enterprise agrees with the Commission that internal network security monitoring would advance Responsible Entities' cyber security posture towards more zero trust architectures.

While the ERO Enterprise considers internal network security monitoring an appropriate approach to address the risks in the NOPR, the ERO Enterprise looks forward to reviewing comments received in response to this NOPR regarding other considerations for standards development. If commenters suggest other methods or approaches may be effective to address the risks, the ERO Enterprise requests the Commission consider incorporating flexibility to consider such methods or approaches in any final rule issued in this proceeding.

B. Due to the complexity of the matter, the ERO Enterprise requests the Commission defer to NERC regarding the timeline for any standards development.

The ERO Enterprise supports the prompt development of standards to address identified reliability risks. Should the Commission determine to issue a final rule directing the development of standards to require internal network security monitoring in this proceeding, the ERO Enterprise respectfully requests that the Commission defer to NERC regarding the appropriate development timeline. As discussed below, there are a number of complex considerations that must be taken into account in developing responsive standards requirements. The reliability and security of the Bulk-Power System ("BPS") would benefit from allowing a comprehensive discussion of these considerations through the NERC standard development process.

There are several considerations that need appropriate time to factor into standards development. Stakeholders will need to consider application of internal network security monitoring, or other methods, to a variety of BES Cyber System configurations or environments. For instance, internal network security monitoring could be challenging for Responsible Entities that group each BES Cyber Asset into a single BES Cyber System, if they choose to continue to group devices as such. The concept of applying a control from one to many is much simpler than controls that would need to be applied one-to-one. Furthermore, stakeholders will need to consider impacts to Real-time operations and industrial control systems or operating technology environments to ensure any issues, such as latency, do not impede necessary functions. In addition to technical considerations, stakeholders will need to consider the scalability and manageability of this approach for Responsible Entities of all sizes.

Moreover, stakeholders would need to consider whether required monitoring is sufficient to address the risk or if additional action is warranted. In the proposed directive, the Commission states that any modifications should factor in the following three security objectives:

> (1) the need for a network traffic baseline based on analysis of network traffic and data flows in order to reduce the likelihood an attacker could exploit legitimate cyber resources;
>
> (2) the need to monitor for and detect unauthorized activity, connections, devices, and software inside the ESP in order to reduce detection time and shorten the timeframe for an attacker to traverse the network; and
>
> (3) the ability to support operations and response by (i) logging and implementing packet capture of network traffic; (ii) maintaining sufficient records for investigations; and (iii) implementing measures to minimize likelihood of an attacker removing any evidence of their tactics, techniques, and procedures.[15]

In considering these objectives, stakeholders would need to determine if monitoring alone is sufficient or if an additional required mitigation measure is appropriate once suspicious activity is

[15] NOPR at P 31.

detected. Mitigation measures, however, would need to factor in reliability, which means reporting and investigation may proceed mitigation. At times, the best interests of reliability or security may be served by not immediately taking certain follow up actions, depending on the availability needs of the system.[16] These considerations are complex and could have wide ranging implications, and as such any language must be carefully considered.

To that end, while the ERO Enterprise intends to act expeditiously to support any directed standards revisions, the ERO Enterprise respectfully requests the Commission not impose deadlines that could hamper thoughtful deliberations on technical considerations, scalability and manageability for Responsible Entities of all sizes, and whether any further implementation requirements may be necessary.

C. The ERO Enterprise supports considering internal network security monitoring for assets containing low impact BES Cyber Systems but notes requiring internal network security monitoring for all low impact BES Cyber Systems could involve extensive revisions to the CIP standards.

While the ERO Enterprise supports internal network security monitoring as an appropriate approach for consideration for high and medium impact BES Cyber Systems, the ERO Enterprise notes that requiring such monitoring for low impact BES Cyber Systems would require extensive revisions to the CIP Reliability Standards and a correspondingly longer period to implement. Current CIP requirements for low impact BES Cyber Systems have several distinct characteristics from those for high and medium that could make consideration of requirements for internal network security monitoring challenging.

First, there are technical and practical considerations for mandating internal network security monitoring for low impact BES Cyber Systems. For instance, there may be technical

[16] *See* Guidelines and Technical Basis in Reliability Standard CIP-007-6, page 44, available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf.

challenges for assets at low impact BES Cyber Systems, based on the diverse implementations of relays, remote terminal units, and communications processors, among others, that would need to be considered. Furthermore, there may be scalability and manageability issues for applying internal network security monitoring to low impact BES Cyber Systems, including considering whether communications paths would need to be enhanced to correct any latency or Real-time operations impact. The ERO Enterprise looks forward to reviewing the comments received from industry stakeholders in this proceeding regarding these types of technical considerations.

Second, CIP standards do not require a list of low impact BES Cyber Systems; rather, controls are applied at the asset containing the low impact BES Cyber Systems. Without a required identification of BES Cyber Systems, it could be difficult to audit application of internal network security monitoring at the device level. Furthermore, there is no ESP as required by CIP-005-6 for low impact BES Cyber Systems. As such, it would be difficult to scope or audit internal network security monitoring for low impact BES Cyber Systems given monitoring should be inside an ESP. If changes to Reliability Standards were contemplated to better facilitate internal network security monitoring requirements, these changes could require significant CIP standards revisions beyond a simple requirement to mandate internal network security monitoring.

In terms of requiring internal network security monitoring for subsets of low impact BES Cyber Systems, the ERO Enterprise notes that the routable connectivity of a low impact BES Cyber System external to its network could pose more of a risk than other configurations. However, this again could take more significant revisions to the CIP standards in terms of identifying and categorizing low impact BES Cyber Systems. Along those lines, NERC standard drafting team Project 2020-03 Supply Chain Low Impact Revisions includes considerations for addressing risks associated to low impact BES Cyber Systems with routable connectivity in its latest draft proposal,

including controls for detecting malicious communications from vendors to low impact BES Cyber Systems.[17]

Should the Commission determine to mandate development of any subset of low impact BES Cyber Systems for required internal network security monitoring, the ERO Enterprise requests the Commission defer to the ERO Enterprise and its stakeholder processes on appropriate subsets, particularly in light of the work being performed to assess low impact BES Cyber Systems. In February 2021, the NERC Board of Trustees directed NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and report on whether those criteria should be modified.[18] To meet this directive, NERC has assembled a team to assess the connectivity of low impact BES Cyber Systems, among other characteristics, and how that connectivity impacts their risk to the BPS if compromised. The ERO Enterprise requests that any subset lists in standards development wait until completion of this group's work. The ERO Enterprise looks forward to reviewing comments received regarding low impact BES Cyber Systems in response to the NOPR.

.

[17] The latest drafts are posted on the Project 2020-03 web page at https://www.nerc.com/pa/Stand/Pages/Project_2020-03_Supply_Chain_Low_Impact_Revisions.aspx.

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

II. CONCLUSION

The ERO Enterprise appreciates the opportunity to comment in this matter. As discussed above, the ERO Enterprise recognizes the risks identified by the Commission and that internal network security monitoring is an appropriate method to address them. The ERO Enterprise looks forward to comments received on the approach and requests the Commission consider any alternatives before adopting the proposed approach. If the Commission adopts the proposal in the NOPR, the ERO Enterprise urges the Commission to defer to the NERC standards development process to determine the appropriate timeframe for developing any revisions. Regarding low impact BES Cyber Systems, internal network security monitoring could require more extensive revisions to the CIP Reliability Standards. Any subset of such systems should factor in the work developed by the NERC team assessing the routable connectivity of low impact BES Cyber Systems. As such, the ERO Enterprise respectfully requests the Commission consider these comments and looks forward to reviewing other comments received in response to this NOPR to determine next steps, if any.

Respectfully submitted,

/s/ Marisa Hecht

/s/ Niki Schaefer
Niki Schaefer
Vice President & General Counsel
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, Ohio 44131
(216) 503-0600
(216) 503-9207 - facsimile
niki.schaefer@rfirst.org
Counsel for ReliabilityFirst Corporation

/s/ Holly A. Hawkins
Holly A. Hawkins
Vice President, General Counsel, and Corporate Secretary

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net
Counsel for the North American Electric Reliability Corporation

SERC Reliability Corporation
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273
(704) 357-7372
hhawkins@serc1.org
Counsel for the SERC Reliability Corporation

/s/ Derrick Davis
Derrick Davis
Vice President, General Counsel & Corporate Secretary
Texas Reliability Entity, Inc.
805 Las Cimas Parkway, Suite 200
Austin, TX 78746
(512) 583-4900
derrick.davis@texasre.org
Counsel for Texas Reliability Entity, Inc.

/s/ Steven F. Goodwill
Steven F. Goodwill
Senior Vice President of Strategic Engagement, General Counsel and Secretary
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6879
sgoodwill@wecc.org
Counsel for the Western Electricity Coordinating Council

/s/ Lisa A. Zell
Lisa A. Zell
Vice President General Counsel and Corporate Secretary
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1760
lisa.zell@mro.net
Counsel for Midwest Reliability Organization

/s/ Damase Hebert
Damase Hebert
Associate General Counsel & Director, Enforcement
Northeast Power Coordinating Council, Inc.
1040 Ave. of the Americas, 10th Floor
New York, NY 10018
(212) 840-1070
dhebert@npcc.org
Counsel for Northeast Power Coordinating Council, Inc.

Date: March 28, 2022