UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security	**)** **)**	**Docket No. RM20-19-000**

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

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's ("FERC" or "Commission") Notice of Inquiry ("NOI")[2] regarding the potential risks to the Bulk Electric System ("BES")[3] posed by the use of telecommunications equipment and services produced or provided by certain entities identified by the United States Congress as risks to national security.[4]

The ERO Enterprise recognizes that there is a risk that adversaries to the United States could leverage the supply chain of equipment and services to exploit potential vulnerabilities and carry out cyber-attacks to disrupt the operation of the Bulk-Power System ("BPS"). In response, the ERO Enterprise has developed a defense-in-depth approach to mitigating supply chain risks through a combination of mandatory and voluntary activities for entities, as described further below. As part of this defense-in-depth approach, the ERO Enterprise has various tools to address

[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] *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, Notice of Inquiry, 172 FERC ¶ 61,224 (2020) [hereinafter NOI].

[3] Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, http://www.nerc.com/files/Glossary_of_Terms.pdf.

[4] In the NOI the Commission notes that the United States Congress identified certain entities, as well as their subsidiaries and affiliates, providing telecommunications equipment or services as risks. NOI at P 3 (citing the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3) (2018) [hereinafter the 2019 NDAA]).

different aspects of supply chain risk management. Some tools are proactive or preventative – e.g., compliance guidance and Reliability Standards help inform or mandate practices to address supply chain risks broadly. Other tools are more reactive to specific threats, vulnerabilities, or events and facilitate more immediate action – e.g., a NERC Alert or an Electricity Information Sharing and Analysis Center ("E-ISAC") bulletin, which can broadcast quickly an identified vulnerability, threat, or risk and guide entities to take additional mitigation measures.

As part of its defense-in-depth approach, NERC's Reliability Standards include a number of requirements that help mitigate supply chain risks, as discussed below. Many of the requirements in the Critical Infrastructure Protection ("CIP") standards designed to directly address supply chain risk management only went into effect very recently on October 1, 2020. The ERO Enterprise has only just begun assessing efficacy of these requirements. Accordingly, it is premature to comment on the adequacy of these CIP standards. The ERO Enterprise will continue to engage in standards effectiveness reviews. In fact, the CIP supply chain risk management requirements are already undergoing revision through several standards development projects to address issues already identified to, among other things, expand the requirements for assets containing low impact BES Cyber Systems to address supply chain risk management. Therefore, the ERO Enterprise respectfully requests the Commission withhold any assessment of the adequacy of relevant standards and decline to direct further assessments until NERC has completed both the supply chain effectiveness review and the study of electronic access controls for assets containing low impact BES Cyber Systems, as discussed below.

While the focus of the NOI is on telecommunications equipment and services from certain foreign manufacturers, use of this branded equipment and services has not been widespread in the BPS based on ERO Enterprise data. In fact, the 2020 State of Reliability Report stated that there

was "minimal exposure of the BPS through branded products from the named Chinese telecommunications and video surveillance manufacturers…."[5] Nonetheless, as described below, NERC published a joint white paper with FERC staff describing a method to identify devices that are potentially unbranded.

The ERO Enterprise initiates activities to address supply chain risks broadly, not only those posed by telecommunications equipment and services from foreign adversaries. Several of the activities and Reliability Standards requirements detailed below seek to mitigate more risks than just that potentially posed by the telecommunications equipment and services that are the subject of the NOI. Nonetheless, the ERO Enterprise's mandatory and voluntary activities described below help to address the risk of compromised or misused telecommunications equipment.

These comments are organized into the following sections: Section I.A describes ERO Enterprise activities focused on equipment and device identification; Section I.B provides detail on Reliability Standards that address the risk of compromised or misused equipment; and Section I.C describes other activities that help mitigate the risk of United States adversaries leveraging potential vulnerabilities. Section II provides a conclusion to these comments.

I. COMMENTS

The Commission issued the NOI in the wake of recent Executive Orders, legislative actions, and other federal agency decisions addressing supply chain risks. In the NOI, the Commission cited several of these actions as prompting its decision to gather more information on the risks of certain telecommunications equipment and services to the reliability of the BES.[6] The

[5] NERC, *2020 State of Reliability Report*, at p. 4 (2020), at https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf.

[6] Specifically, the Commission noted that two Executive Orders addressed the risk posed by equipment and services from foreign adversaries. NOI at PP 5-8 (citing Executive Order No. 13,873 of May 15, 2019, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689 (May 17, 2019); Executive Order 13,920 of May 1, 2020, *Securing the United States Bulk-Power System*, 85 Fed. Reg. 26595 (May

Commission noted that all these actions, in combination with a report issued by the Defense Innovation Board,[7] support its decision to issue the NOI to further investigate the risks to the BES of telecommunications equipment and services from companies linked to foreign adversaries.

The Commission structures its inquiry into five questions and subparts, labeled by question number (e.g., Q1, Q2, etc.).[8] Specifically, the Commission seeks comment on the following areas: (1) the extent of the use of telecommunications equipment and services provided by certain foreign entities identified as risks to national security related to BES operations; (2) the risks to BES reliability and security posed by the use of equipment and services provided by the identified entities; (3) whether the CIP Reliability Standards requirements adequately mitigate the identified risks; (4) strategies that entities have implemented or plan to implement – in addition to compliance with the mandatory CIP Reliability Standards – to mitigate the risks associated with use of equipment and services provided by the identified entities; and (5) other methods the Commission may employ to address this matter, including working collaboratively with industry to raise awareness about the identified risks and assisting with mitigating actions (i.e., such as facilitating information sharing).[9]

4, 2020)). The Commission also cited recent National Defense Authorization Acts, such as the 2019 NDAA, as barring certain federal departments from using or procuring certain equipment, particularly from Huawei or ZTE Corporation, deemed "Covered Companies." NOI at PP 9-11 (citing National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1656 (2017) and the 2019 NDAA). Finally, the Commission also cited two Federal Communications Commission orders designating both Huawei and ZTE Corporation as covered entities that are prohibited from Universal Service Fund money to support the purchase of any equipment or services provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain. NOI at P 12 (citing Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation, PS Docket No. 19-351, Order (Jun. 30, 2020); Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation, PS Docket No. 19-352, Order (Jun. 30, 2020)).

7 NOI at P 14 (citing The 5G Ecosystem: Risks and Opportunities for DoD, Defense Innovation Board (Apr. 3, 2019), https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF).

8 NOI, *supra*, at P 20.

9 NOI, *supra*, at P 4.

In these comments, the ERO Enterprise addresses these questions as follows: Section I.A. addresses Question Q1 by describing ERO Enterprise activities designed to assess the extent certain telecommunications equipment and services are used in the BES; Section I.B. addresses Questions Q2 and Q3 by describing the controls in the NERC Reliability Standards that help mitigate the risk; and Section I.C. addresses Questions Q4 and Q5 by describing other activities designed to help mitigate the risk.

A. ERO Enterprise recognizes the importance of managing supply chain risks and supports entities in identifying equipment and services that present heightened risks to the BPS as a result of their supply chain.

The ERO Enterprise recognizes the importance of supply chain risk management and the threat that compromised equipment and services present to the BPS. NERC's 2020 State of Reliability Report identified supply chain compromise as an attack vector that could be used by adversaries.[10] That report noted that "[a]n adversary's goal in supply chain compromise is getting a specific organization or industry to acquire and use equipment that has unknown exploitable features."[11]

In recognition of supply chain risks to BPS security, the ERO Enterprise works with entities to support their supply chain risk management activities. One important component of risk assessment is identifying the manufacturers and suppliers of the infrastructure and systems that make up the BPS and assessing whether they present risks to reliable and secure operations. To support this objective, the ERO Enterprise has developed several Alerts, and a white paper jointly with FERC staff, as described in more detail below.

[10] 2020 State of Reliability Report, at p. 78.
[11] *Id.*

1. Level 2 Alerts

Over the past few years, NERC has issued non-public Level 2 Alerts to raise awareness of specific threats posed by foreign manufactured equipment and software. To effectively disseminate this information, NERC issues email-based Alerts designed to provide concise, actionable information to the electricity industry.[12] NERC uses the Alert responses to assess the extent of exposure of the BPS to certain identified risks. A high-level description of each of these three Level 2 Alerts is provided below.

Level 2 Alert regarding Kaspersky Anti-Virus Software: In October 2017, NERC issued a non-public Level 2 Alert regarding supply chain risk, specifically stakeholders' use of Kaspersky anti-virus software. Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on systems using their products and can be exploited by malicious cyber actors to compromise those systems.

Level 2 Alert regarding Telecommunications Equipment Manufactured by Certain Chinese Companies: In July 2019, NERC issued a non-public Level 2 Alert to raise awareness among NERC registered entities of persistent supply chain risks related to certain Chinese manufacturers of telecommunication equipment and to request information to assess the extent of exposure of the BPS to these risks. This Alert was in response to the 2019 NDAA identifying certain "Covered Companies" and addresses the risk identified in the NOI. Consistent with NERC Rules of Procedure Section 810, NERC provided a report to the Commission describing the actions taken

[12] As defined in NERC Rules of Procedure Section 810, NERC Alerts are divided into three distinct levels, as follows: (1) Industry Advisory: Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary; (2) Recommendation to Industry: Recommends specific action be taken by registered entities. A response from recipients, as defined in the alert, is required; and (3) Essential Action: Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees' approval prior to issuance. Like recommendations, essential actions also require recipients to respond as defined in the alert. The NERC Rules of Procedure are available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20190125.pdf.

by entities who responded to the Alert. Based on the responses received, the 2020 State of Reliability Report stated the following:

> Analysis of the responses suggest minimal exposure of the BPS through branded products from the named Chinese telecommunications and video surveillance manufacturers and a somewhat more common use of Chinese manufactured or supplied unmanned aerial systems (UASs) for maintenance or asset management activities.[13]

Level 2 Alert regarding May 2020 Executive Order: In July 2020, NERC issued a non-public Level 2 Alert requiring registered entities to report on equipment used that is banned by an Executive Order issued concerning security of the BPS.[14] Consistent with NERC Rules of Procedure Section 810, NERC provided a report to the Commission describing the actions taken by entities who responded to the Alert.

2. Joint White Paper on Supply Chain Vendor Identification

In 2020, NERC worked with FERC staff to develop a joint white paper on supply chain vendor identification to assist entities in identification of devices, including those from foreign manufacturers.[15] The white paper provides techniques entities may use to noninvasively identify the network interface controller ("NIC").

While the techniques described in the white paper will aid in identifying the NIC vendor, the ERO Enterprise notes that the presence of certain equipment does not necessarily indicate malicious activity. If a vendor of concern is identified, it does not confirm there is malicious activity in the network. Rather, actions should be taken to determine if the device or component

---

[13] 2020 State of Reliability Report at p. 4.

[14] Executive Order 13920 of May 1, 2020, *Securing the United States Bulk-Power System*, 85 Fed. Reg. 26595 (May 4, 2020).

[15] 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.

exhibits malicious activity. The techniques in the white paper are designed to be noninvasive, thereby reducing the risk of impacts to BES reliability, but entities are encouraged to assess their own environment to determine the risk of interruption of communications.

Using tools such as the Level 2 Alerts and joint white paper, the ERO Enterprise is actively engaged in assisting industry to assess the equipment and services used by their organization and the potential for any vulnerabilities or threats.

B. NERC Reliability Standards help to address the risk posed by potential compromise of telecommunications equipment and services.

Existing and future NERC Reliability Standards help address the supply chain risks, including those posed by potential compromises to telecommunications equipment and services. The Reliability Standards that address supply chain risk management most directly, however, just became effective in the United States on October 1, 2020, making comment on their effectiveness premature at this time. While the ERO Enterprise cannot yet comment as effectiveness reviews are ongoing, other NERC Reliability Standards that have been effective longer help address the risk by placing protections around BES Cyber Systems and other applicable systems.

1. Supply Chain Standards and Requirements

Recently, new and revised requirements addressing supply chain risk management became effective in the United States. These requirements aim to mitigate risks posed by compromised equipment or services, including those compromised by malicious actors, prior to or during the procurement process. The following is an overview of those standards and requirements:

- CIP-013-1: Reliability Standard CIP-013-1 requires Responsible Entities to develop and implement plans to address supply chain cybersecurity risks during the planning and procurement of high and medium impact BES Cyber Systems. As stated in the petition for approval, the security objective of the supply chain cybersecurity risk management plans is to ensure that Responsible Entities consider the security, integrity, quality, and resilience of the supply chain and take appropriate mitigating action when procuring BES Cyber Systems to address

threats and vulnerabilities in the supply chain.[16] Should products or services from a particular vendor be identified as potentially posing a risk, Responsible Entities would be expected to consider that risk during the planning and procurement process.

- CIP-005-6, Requirement R2, Parts 2.4 and 2.5: Pursuant to Requirement R2, Parts 2.4 and 2.5 of Reliability Standard CIP-005-6, Responsible Entities must have one or more methods for: (1) determining active vendor remote access sessions (Part 2.4); and (2) disabling active vendor remote access (Part 2.5).[17] The security objective of these requirement parts is to control vendor remote access to mitigate risks associated with unauthorized access.[18]

- CIP-010-3, Requirement R1, Part 1.6: CIP-010-3 Requirement R1, Part 1.6 requires Responsible Entities to verify the integrity of the software (such as patches) obtained from the software source prior to a change deviating from the baseline configuration.

- Low impact BES Cyber Systems: For low impact BES Cyber Systems, future standards revisions will address supply chain cyber security risks. Project 2020-03 – Supply Chain Low Impact Revisions will consider the recommendations outlined in the Supply Chain Risk Assessment Report. Specifically, the project will include revisions to CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

As noted previously, these Reliability Standards only recently became effective on October 1, 2020. The ERO Enterprise is actively assessing efficacy of these standards as part of the Supply Chain Risk Mitigation Program.[19] This plan details how the ERO Enterprise will measure the effectiveness of the supply chain standards during the first two years of implementation. At a high level, the plan includes the following actions: (1) surveys on supply chain awareness to inform analysis of trends; (2) comparison of contract language provided voluntarily by entities; (3) review

[16] *Petition of NERC for Approval of Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, Docket No. RM17-13-000, p. 13 (Sep. 26, 2017) ("NERC Petition").
[17] *Id.*
[18] *Id.*
[19] NERC, *Plan to Evaluate Effectiveness of Supply Chain Standards* (December 16, 2019), at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Plan%20to%20Evaluate%20Effectiveness%20of%20Supply%20Chain%20Standards.pdf.

of audit and compliance information to determine whether language is clear or whether there are any reliability gaps; and (4) evaluation of successful communication of supply chain vulnerabilities. NERC staff plans to report to the NERC Board of Trustees periodically on these activities during the first two years of implementation, as necessary. As the supply chain standards only went into effect on October 1, 2020 in the United States, the ERO Enterprise has only just started the two-year time period this plan covers. Therefore, the ERO Enterprise is not yet able to comment on the effectiveness of these standards.

2. Other CIP Reliability Standards and Requirements

NERC CIP Reliability Standards have undergone a transformation over the past several years and continue to progress based on experience with the standards and evolving understanding of risk. Beginning with implementation of the CIP Version 5 standards in 2016, entities have implemented several new requirements that expand security protections.[20] NERC continues to work with industry subject matter experts to revise the CIP Reliability Standards to strengthen their efficacy. The entire suite of CIP Reliability Standards seeks to address the risk posed by compromised or misused existing equipment and services in a risk-based manner. The following describes briefly some of the CIP Reliability Standards and requirements that help to mitigate the risk posed by compromised telecommunications equipment and services:[21]

- CIP-002-5.1a: Reliability Standard CIP-002-5.1a includes the criteria for BES Cyber System categorization, indicating which BES Cyber Systems if lost or compromised would cause the largest impact on the reliability of the BES. Once categorized under CIP-002-5.1a, BES Cyber Systems then receive the protections commensurate with their risk level according to the remainder of the CIP cyber security Reliability Standards.

[20] The suite of standards referred to as CIP Version 5 include the following standards and their successor versions: CIP-002-5.1a, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1.

[21] The ERO Enterprise notes that under several CIP Reliability Standards, Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters are excluded from applicability.

- CIP-005-6: Reliability Standard CIP-005-6 focuses on electronic access controls for high and medium impact BES Cyber Systems and associated applicable systems. These requirements include methods to determine and disable active vendor remote access sessions and directing communications through an Electronic Access Point and methods for detecting known or suspected malicious communications for both inbound and outbound communications. This helps prevent network-based attacks by controlling what devices can communicate with applicable BES Cyber Systems and associated systems.

- CIP-007-6: CIP-007-6 requires management of ports and services and methods to deter, detect, or prevent malicious code. Furthermore, Responsible Entities must log detected successful and failed login attempts and failed access attempts at the BES Cyber System level or the Cyber Asset level, including Electronic Access Control or Monitoring Systems ("EACMS") associated with medium and high impact BES Cyber Systems, depending on system or device capability.

- CIP-008-6: Should Responsible Entities discover an attempt or actual compromise through their event monitoring, Reliability Standard CIP-008-6, which will become effective in the United States on January 1, 2021, requires mandatory reporting of Cyber Security Incidents, including compromises or attempts to compromise BES Cyber Systems or their associated Electronic Security Perimeters or EACMS.

- CIP-009-6: Should the misuse or compromise of BES Cyber Systems result in the need for recovery and restoration, the requirements in CIP-009-6 include backup and storage processes. CIP-009-6 requires Responsible Entities to have, implement, and maintain recovery plans for medium and high impact BES Cyber Systems and their associated EACMS and Physical Access Control Systems ("PACS") at Control Centers. Recovery of these systems helps to support the availability of information critical to the restoration of BES Cyber Systems.

- CIP-010-3: CIP-010-3 addresses configuration change management. [22] Specifically, CIP-010-3, Requirement R1 requires Responsible Entities to develop a baseline configuration for certain firmware or software and authorize any changes that deviate from the existing baseline configuration for high and medium BES Cyber Systems and their associated EACMS, PACS, and Protected Cyber Assets ("PCAs"). CIP-010-3, Requirement R2, Part 2.1 requires monitoring high impact BES Cyber Systems and their associated EACMS and PCAs for changes, including unauthorized changes.

[22] The National Institute of Standards and Technology ("NIST") defines Configuration Management as "A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle." *Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations* app. B, at B-5 (2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

- CIP-012-1: Reliability Standard CIP-012-1 requires Responsible Entities to develop a plan to mitigate the risks posed by unauthorized modification (integrity) and unauthorized disclosure (confidentiality) of Real-time Assessment and Real-time monitoring data transmitted between Control Centers, including over telecommunications links. Additionally, Project 2020-04 is developing revisions to CIP-012-1 to address the availability of communications links and data communicated between BES Control Centers, consistent with Order No. 866.[23]

Similar to the supply chain Reliability Standards, the ERO Enterprise is assessing the efficacy of electronic access controls contained in the CIP standards for assets containing low impact BES Cyber Systems. This effort is in response to a Commission directive issued in Order No. 843, with a regulatory deadline of filing NERC's analysis with the Commission by July 1, 2021.[24] The results of this study will provide input on how effective these controls are at protecting low impact BES Cyber Systems. As a result, the ERO Enterprise declines to comment until the analysis of these controls has been completed. At such time, the ERO Enterprise will file the report as directed by July 1, 2021.

3. Reliability Standards Addressing the Operation and Planning of the BPS

Finally, NERC Reliability Standards focusing on operations and planning also contribute to mitigating the risk should telecommunications equipment become compromised:

- IRO-002-5 and TOP-001-4: Reliability Standards IRO-002-5 and TOP-001-4 require Reliability Coordinators ("RCs"), Balancing Authorities ("BAs"), and Transmission Operators ("TOPs") to have redundant and diversely routed data exchange infrastructure for Real-time Assessment and Real-time monitoring data within a primary Control Center.

- COM-001-3: Reliability Standard COM-001-3 requires RCs, BAs, and TOPs to have alternative interpersonal communication capability, which could be used if there is a suspected compromise of oral communication on one channel.

- EOP-008-2: Reliability Standard EOP-008-2 requires RCs to have backup Control Center facilities, or backup Control Center functionality for BAs and TOPs, in

[23] *Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers*, Order No. 866, 170 FERC ¶ 61,031 (2020).

[24] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Order No. 843, 163 FERC ¶ 61,032 at P 30 (2018).

> addition to their primary Control Centers. Moreover, RCs, BAs, and TOPs must consider physical and cyber security as an element of their Operating Plan for backup functionality. These requirements help to ensure that there are alternate paths for communicating should one be compromised.

Each of the requirements detailed in this section play a key role in helping to address risks, including those posed by compromised telecommunications equipment. Whether by providing additional communication capabilities or requiring protections for BES Cyber Systems from malicious actors, these requirements help maintain reliable operations of the BES should certain components fail. As noted above, the ERO Enterprise is in the process of completing further review and study of the effectiveness of the supply chain Reliability Standards and the study of electronic access controls for assets containing low impact BES Cyber Systems, and is not yet able to comment on the effectiveness of these standards. NERC respectfully requests the Commission allow NERC to complete these assessments before directing further assessments of the efficacy of these standards with respect to the risks posed by compromised telecommunications equipment.

C. The ERO Enterprise supports activities beyond mandatory Reliability Standards to help industry mitigate risk should equipment or services be compromised.

The ERO Enterprise takes a defense-in-depth approach by engaging in activities in addition to mandatory Reliability Standards to help industry mitigate cyber security risks. While mandatory Reliability Standards play an integral role in securing the BPS, the ERO Enterprise recognizes the importance of multiple approaches in supporting cyber security risk mitigation. These efforts include the Level 2 Alerts and white paper regarding identification and assessment of equipment and services, as discussed in Section I.A. The ERO Enterprise's efforts also include an initiative dedicated to supply chain risk mitigation, information sharing, industry outreach, and collaboration with industry stakeholders. Each of these efforts is described in detail below.

1. The Supply Chain Risk Mitigation Program

In addition to supporting the implementation of the supply chain standards, the Supply Chain Risk Mitigation Program, adopted as resolutions by the NERC Board of Trustees, includes the following efforts to enhance reliability through mitigation of supply chain risks:

1. Performed cyber security supply chain risk study and engaged the Electric Power Research Institute to perform an independent assessment of supply chain risks;

2. Communicates supply chain risks to industry;

3. Requested forums and trade associations to develop white papers addressing best and leading practices for supply chain management; and

4. Evaluates the effectiveness of supply chain standards.

Consistent with the defense-in-depth approach to cyber security, the ERO Enterprise recognizes direct engagement with industry groups enhances risk mitigation activities. For instance, the NERC Board of Trustees requested the North American Transmission Forum ("NATF") and the North American Generation Forum to develop white papers to address best and leading practices in supply chain management.[25] In response, the NATF developed and published for general industry use a method for entities to evaluate suppliers' cyber security practices, including a set of criteria and an associated questionnaire.[26] These criteria and the associated questionnaire incorporate the applicable NERC standards and map to existing frameworks, such

[25] NERC Board of Trustees, *Minutes — Board of Trustees* (Aug. 10, 2017) at 10, https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/BOT%20-%20August%2010%202017%20Minutes.pdf.

[26] NATF, *Cyber Security Criteria for Suppliers*, (Jan. 31, 2020), https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-cyber-security-criteria-for-suppliers.xlsx; NATF, *Supplier Cyber Security Assessment Model* (Jan. 31, 2020), https://www.natf.net/docs/natf/documents/resources/supply-chain/supplier-cyber-security-assessment-model.pdf; NATF, *Energy Sector Supply Chain Risk Questionnaire – Formatted* (May 7, 2020), https://www.natf.net/docs/natf/documents/resources/supply-chain/energy-sector-supply-chain-risk-questionnaire---formatted.xlsx.

as the NIST Framework, in use by the vendor community.[27] In applying the criteria, entities collect and verify information from suppliers and identify and evaluate supplier risk. The process then provides for entities to determine what risk can be mitigated and whether any risk can be accepted; make a purchase with appropriate contract provisions to reinforce mitigation; and then implement an ongoing process to monitor additional risk. These criteria support entities in evaluating and identifying the risk posed and developing appropriate mitigation prior to making a purchase. The ERO Enterprise has observed that entities, suppliers, and third-party assessors are beginning to adopt the NATF criteria, questionnaire, and other associated tools. Recognizing the importance of information sharing for supply chain risk mitigation, the NATF has made these criteria available to all of industry.[28]

2. Information Sharing through the E-ISAC

Critical to the mitigation of any risks posed by certain products and services is the timely communication of any threats and vulnerabilities. The E-ISAC plays a central role in this communication. Information sharing in near real-time provides a key component in mitigating risk, particularly those posed by a malicious actor leveraging compromised equipment or services as an attack vector. Using information shared by industry participants and government and cross-sector partners, the E-ISAC informs industry of potential threats or vulnerabilities to the security of the grid to help industry mitigate impacts in a timely manner. Should the E-ISAC identify a supply chain risk, including vulnerability with certain telecommunications equipment or services, the E-ISAC would share the information broadly and quickly to provide context relevant to the electric industry.

[27] NATF, *Cyber Security Criteria for Suppliers*, *supra*.

[28] NATF developed a public-facing webpage on supply chain cyber security industry coordination, https://www.natf.net/industry-initiatives/supply-chain-industry-coordination (last visited Aug. 21, 2020).

For example, the E-ISAC highlights critical vulnerabilities and patches that may require immediate patching based on a variety of government and private sector security sources, giving these critical patches weighted importance over other more routine events. E-ISAC analysts provide additional context specific to the electricity industry using a variety of sources, and then communicate this information through Cyber Bulletins, All Points Bulletins, or Critical Broadcast Program calls, as necessary. An example of this was the recent disclosures of the Ripple20, Microsoft Domain Name System Servers, and the Citrix ADC vulnerabilities. In some cases, E-ISAC posted awareness and mitigation instructions prior to the vulnerabilities being listed in the NIST National Vulnerability Database. E-ISAC analysts posted this information to the E-ISAC Portal, and shared with critical stakeholders in government and the Electricity Subsector Coordinating Council to ensure broadest possible awareness. This sharing permits industry to learn of and address vulnerabilities quickly should equipment or services be compromised or misused.

The E-ISAC routinely posts cyber security and news bulletins related to vulnerability disclosures of equipment and software used by the electricity industry and provides additional context on the impact to the grid, as well as mitigation best practices. Member utilities can review the information and ask follow-up questions of E-ISAC analysts and other utilities through the E-ISAC Portal. The E-ISAC has also hosted webinars and Critical Broadcast Program calls related to major vulnerability disclosures enabling, in some cases, the vendor to speak directly to the electricity industry about the vulnerability or breach, as well as possible mitigations. E-ISAC analysts, member utilities, and vendors are encouraged to use the NIST Framework when describing their vulnerabilities and mitigations to further enhance response, as well as the MITRE ATT&CK® Frameworks for describing the cyber security tactics and techniques observed by adversaries in both enterprise and industrial control system networks.

Additionally, the E-ISAC administers, in coordination with the Department of Energy ("DOE") and the Pacific Northwest National Laboratory ("PNNL"), the Cybersecurity Risk Information Sharing Program ("CRISP"). CRISP provides a two-way exchange of unclassified and classified threat information affecting the energy sector. Data shared through the CRISP program is near-real-time, with analysts at DOE and PNNL providing identification of threat patterns and attack indicators across the energy industry.

Moreover, the E-ISAC runs the GridEx, a biennial exercise, to test the ability of the grid to respond to coordinated cyber and physical attacks. The focus of GridEx is continent-wide, with scenarios designed to validate and exercise industry-wide maturation and improvements from previous GridEx exercises, and to explore the ramifications of new policy and technological developments, to promote learning. NERC is committed to enhancing the GridEx program to meet the challenges posed by the ever-evolving threat environment. In the most recent GridEx V Executive Tabletop, discussion focused on unity of effort with interdependent sectors, such as telecommunications and natural gas. The lessons learned report recommended industry "enhance coordination with communications providers to support restoration and recovery and advocate for continued availability of GHz spectrum" to support mitigation efforts if equipment or services were compromised.[29] The report also recommended that industry "identify key supply chain elements and consider the formation of shared inventory programs for the most critical components" based on a scenario inject that posited a compromise of key and pervasive grid components and the need for large-scale mitigation.[30] GridEx provides a critical forum for industry

[29] NERC and E-ISAC, *GridEx V, Grid Security Exercise: Lessons Learned Report*, at p. 8 (Mar. 2020), at https://www.eisac.com/cartella/Asset/00008427/TLP_WHITE_GridEx_V_Public_After_Action_Report.pdf?parent=123814.

[30] *Id.* at p. 10.

to share information, exercise response and recovery, and identify future threats to enhance overall resilience.

3. Stakeholder Engagement

The ERO Enterprise also recognizes facilitating collaboration with industry as essential to identifying and mitigating risk. In addition, NERC's committees are identifying and developing mitigation approaches for supply chain risks. In the Reliability Issue Steering Committee's ("RISC's") biennial ERO Reliability Risk Priorities Report, the RISC recommended development of supply chain cyber security superior practices as a mitigation activity.[31] Further, NERC recently formed the Reliability and Security Technical Committee ("RSTC"), consolidating all NERC committees focused on technical subject matter into one committee. This approach recognizes the need for security considerations during all operations and planning activities. For example, rather than separating cyber and physical security subgroups from operations and planning subgroups, the RSTC is considering ways in which all of its subgroups can incorporate cyber and physical activities into their work.[32]

Similarly, in light of the evolving nature of threats to the BPS, the ERO Enterprise adjusts its business operations as needed to appropriately assess risk. For example, NERC has recently formed the BPS Security and Grid Transformation department that is focusing on ways in which industry can further integrate physical and cyber security aspects into conventional planning, operations, design, and system restoration activities. As the North American BPS continues to evolve in terms of its resource mix and technologies being utilized in operational technology,

[31] NERC RISC, *2019 ERO Reliability Risk Priorities Report*, at p. 23 (Nov. 2019), at https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20ERO%20Priorities%20Report_Board_Accpeted_November_5_2019.pdf.

[32] NERC Reliability and Security Technical Committee, Agenda Item 3 (October 14, 2020), at https://www.nerc.com/comm/RSTC/AgendaHighlightsandMinutes/RSTC_Special_Meeting_October_14_2020_Agenda_Package_PUBLIC_POSTING.pdf.

information technology, and industrial controls systems, it is critical for security considerations to be at the forefront of engineering and business decisions. The BPS Security and Grid Transformation department will work with the RSTC and its technical sub-groups, government partners, national labs, academia, suppliers, and vendors to engage industry experts toward planning and operating a system that is reliable and cyber resilient.

The ERO Enterprise also engages in outreach regarding risk mitigation with relevant stakeholders. The ERO Enterprise hosts webinars and workshops, develops lessons learned documents, and performs assist visits with entities. The ERO Enterprise offers these activities at a continent-wide level as well as a regional level.

As suggested by the NOI, there may be a number of ways to address the risks to reliability posed by compromised telecommunications equipment and services. The ERO Enterprise employs a comprehensive approach to accomplish its mission of maintaining a reliable BPS in the face of cyber security threats, including mandatory Reliability Standards, Alerts, information sharing, and stakeholder outreach through committees and programs. Should NERC identify additional risks and potential solutions to mitigate them, such as Reliability Standards revisions, NERC would review and take action through its open and inclusive stakeholder process.

II. CONCLUSION

As discussed above, the ERO Enterprise supports Responsible Entities in assessing telecommunications equipment and services to identify risks posed. The ERO Enterprise continues to work with industry, through standards development projects and other activities, to help ensure the risks described above are addressed and mitigated if needed.

Respectfully submitted,

/s/ Marisa Hecht

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

Date: November 23, 2020