UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Potential Enhancements to the Critical Infrastructure Protection Reliability Standards	**)** **)** **)**	**Docket No. RM20-12-000**

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") regarding potential enhancements to the Critical Infrastructure Protection ("CIP") Reliability Standards.[2] Specifically, the Commission seeks comment on (1) whether certain subcategories from the National Institute of Standards and Technology ("NIST") Cybersecurity Framework[3] ("NIST Framework") are adequately addressed by the CIP Reliability Standards; and (2) the potential risk of a coordinated cyber attack on geographically distributed targets and whether modifications to the CIP Reliability Standards would be appropriate to address such risk.

The ERO Enterprise supports continued efforts to strengthen the cyber security posture of Responsible Entities to enhance reliability and resilience against cyber attacks.[4] The ERO

---

[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] *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, Notice of Inquiry, 171 FERC ¶ 61,215 (2020) [hereinafter NOI].

[3] The NIST Cybersecurity Framework provides a structure to guide cyber security activities and to consider cyber security risks as part of an organization's risk management processes of its critical infrastructure. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [hereinafter NIST Framework].

[4] 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.

Enterprise recognizes the evolving nature of cyber security threats and employs a defense-in-depth approach to address vulnerabilities and mitigate risk. NERC has new and modified CIP Reliability Standards in various stages of implementation that will strengthen the requirements already in effect. NERC is also in the midst of several standards development projects aimed at enhancing the CIP Reliability Standards to provide additional protection against cyber threats and vulnerabilities.[5] Moreover, the ERO Enterprise engages in activities beyond Reliability Standards designed to help identify and mitigate security risks. For example, NERC operates the Electricity Information Sharing and Analysis Center ("E-ISAC"), whose mission is to promote information sharing among Responsible Entities and other sectors to help identify threats and mitigating measures. While the ERO Enterprise demonstrates continued adaptability in response to emerging threats, the ERO Enterprise appreciates the Commission's continued efforts to facilitate discussion on potential enhancements to NERC's CIP Reliability Standards.

In the comments below, the ERO Enterprise describes how the current CIP Reliability Standards, in combination with CIP Reliability Standards coming into effect, those in development, and non-standards activities, address the areas in the NIST Framework identified by the Commission in the NOI. The ERO Enterprise emphasizes its continued reliance on the NIST Framework to inform its cyber security activities, including standards development and efforts to support effective implementation of enforceable Reliability Standards. The NIST Framework and the CIP Reliability Standards serve different purposes, however. Whereas the NIST Framework is

[5] NERC CIP Reliability Standards development projects address the following topics: (1) virtualized technologies, (2) supply chain risk mitigation for Electronic Access Control or Monitoring Systems and Physical Access Control Systems, (3) supply chain risk mitigation for low impact BES Cyber Systems, (4) BES Cyber System Information access management, (5) revisions to CIP-012-1 to address availability of data and communications links between Control Centers, and (6) a CIP Standards Efficiency Review project. Each of these efforts uses concepts from the NIST Framework to help develop controls, as appropriate, for mandatory requirements. Information on the current standards development projects is available at https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx.

voluntary guidance, the NERC CIP Reliability Standards are mandatory and enforceable for Responsible Entities. The ERO Enterprise uses concepts from the NIST Framework that are suited to developing mandatory and auditable CIP requirements. For example, the CIP "Version 5" standards drew concepts from the NIST Framework.[6] As such, there will not be a complete overlap from the voluntary framework to the mandatory requirements. Nonetheless, the ERO Enterprise's effort, in coordination with NIST, to map the CIP standards to the NIST Framework indicates that there is significant alignment between the controls within the CIP Reliability Standards and the controls within the NIST Framework. Moreover, the ERO Enterprise engages in many non-standards activities that draw from the NIST Framework to support Bulk-Power System security and reliability.

The ERO Enterprise also discusses its focus on assessing the emerging risk of a coordinated cyber attack against dispersed geographical targets and activities designed to mitigate the risk. As described below, the existing efforts of the ERO Enterprise help to mitigate risks to the reliable operation of the Bulk Electric System ("BES"). These efforts consist of a combination of mandatory Reliability Standards and information sharing through reports, assessments, alerts, and other activities to promote situational awareness. The ERO Enterprise continually seeks to improve its Reliability Standards and other activities and will consider the comments received in this docket in determining next steps, if necessary.

These comments are organized into the following sections: Section I.A provides the ERO Enterprise comments on the NIST Framework and Section I.B provides the ERO Enterprise comments on the risk of a coordinated cyber attack on geographically distributed targets. Section

[6] *See* Docket No. RM13-5-000. In addition to drawing from the NIST Framework, standards drafting teams also rely on special publications from NIST. For example, standard drafting teams often review controls suggested in NIST Special Publication 800-53 when developing requirements.

II provides a conclusion to these comments.

I. COMMENTS

As noted above, the Commission's NOI focuses on two issues: (1) whether certain subcategories from the NIST Framework are adequately addressed by the CIP Reliability Standards; and (2) whether the CIP Reliability Standards appropriately address the risk of a coordinated cyber attack against dispersed geographical targets.

With respect to the NIST Framework, the NOI provides that Commission staff identified three areas which may not be adequately addressed in the CIP Reliability Standards or are addressed only with regard to medium and high impact BES Cyber Systems but not low impact BES Cyber Systems: data security, detection of anomalies and events, and mitigation of cyber security events.[7] Based on this analysis, the NOI seeks comment on certain Subcategories within those three Categories of the NIST Framework and whether the CIP Reliability Standards adequately address them.[8] If commenters indicate inadequacies in the above three areas, the Commission seeks comment on whether these pose a risk to the reliable operation of the Bulk-Power System now and in the future.

Regarding the potential risk of a coordinated cyber attack on geographically distributed targets, the Commission seeks comment on the procedures, processes, and security controls that are currently employed to protect against the potential risk of a geographically distributed coordinated cyber attack and whether these procedures, processes, and controls should be included in the CIP Reliability Standards. Furthermore, the Commission seeks comments on (1) whether any changes to the BES design could impact these risks; (2) whether current drill exercises,

---

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

[8] In the NOI, these questions are labeled as A1, A2, and A3.

training, and industry information sharing are effective in mitigation preparation; and (3) whether the thresholds in the criteria for identifying medium impact BES Cyber Systems in Reliability Standard CIP-002-5.1a are appropriate for addressing the risk of a geographically distributed coordinated attack.[9]

A. The ERO Enterprise consistently relies upon the NIST Framework to inform its cyber security activities.

i. ERO Enterprise Mapping

The ERO Enterprise recognizes the importance of the NIST Framework and works to ensure the NIST Framework's voluntary guidance is taken into consideration and tracked to all mandatory CIP Reliability Standards. As noted in the NOI, the NIST Framework "sets forth a comprehensive, repeatable structure to guide cybersecurity activities and to consider cybersecurity risks as part of an organization's risk management processes of its critical infrastructure."[10] The Commission further noted that there are 5 Functions, [11] with 23 Categories and 108 Subcategories.[12] The Functions relate to the strategic view of an organization's risk management; the Categories cover the cyber security objectives for an organization; and the Subcategories include outcome-driven statements that inform an organization's cyber security program.[13]

Recently, ERO Enterprise staff and NIST staff, with contributions from a working group of NERC's Reliability and Security Technical Committee ("RSTC"), developed an updated mapping of the currently enforceable CIP Reliability Standards to the NIST Framework.[14] NERC

---

9 In the NOI, the questions on coordinated cyber attacks are labeled as B1, B2, B3, B4, B5, B6, and B7.

10 NOI at P 3.

11 The terms Functions, Categories, and Subcategories come from the NIST Framework.

12 NOI at PP 8-9.

13 NIST, *An Introduction to the Components of the Framework* (updated 2020), https://www.nist.gov/cyberframework/online-learning/components-framework.

14 The full mapping is available at https://www.nerc.com/pa/comp/CAOneStopShop/NIST%20CSF%20v1.1%20to%20NERC%20CIP%20FINAL.XLSX.

and NIST staff observed a consistent mapping between CIP Reliability Standards and the NIST Framework. As provided in that mapping document, the NIST Categories identified in the NOI (Data Security, Anomalies and Events, and Mitigation) are mapped to requirements within the CIP Reliability Standards, as further described below. In addition, NERC's Operations and Planning Reliability Standards and CIP Reliability Standards in development demonstrate how the NERC Reliability Standards address the areas identified by the Commission in the NOI. Each Category (Data Security, Anomalies and Events, and Mitigation) is addressed separately below.

a. Data Security

In the NIST Framework, the Data Security Category includes the objective that "Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information."[15] Within the Data Security Category, there are two Subcategories identified by the Commission for further consideration as the subject of the NOI: (1) PR.DS.4 – Adequate capacity to ensure availability is maintained; and (2) PR.DS-6 – Integrity checking mechanisms are used to verify software, firmware, and information integrity.[16] The following section describes how NERC Reliability Standards address PR.DS-4 and PR.DS-6.

PR.DS-4: The Commission states that CIP-011-2 does not address adequate capacity to ensure data availability is maintained and states that CIP-012-1 addresses only the availability of Real-time Assessment and monitoring data transmitted between Control Centers and not the availability of BES Cyber System Information.[17] However, the ERO Enterprise identified other

15 NIST Framework 32.
16 NOI at PP 12-13.
17 *Id.*

Reliability Standards with controls that support adequate capacity to ensure availability is maintained, as described below.

In the NOI, the Commission notes that its concern regarding availability of information includes "[t]he loss of BES Cyber System information availability could result in a loss of the ability to accurately maintain or restore the [BES], which could affect reliability."[18] However, the requirements in CIP-009-6 directly support availability of information used to restore BES Cyber Systems through 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 Electronic Access Control or Monitoring Systems ("EACMS") and Physical Access Control Systems ("PACS") at Control Centers. Specifically, Part 1.3 requires Responsible Entities to include in the recovery plan "[o]ne or more processes for the backup and storage of information required to recover BES Cyber System functionality."[19] Other requirements within CIP-009-6 require Responsible Entities to verify backup completion and test a sample of information or actually recover a BES Cyber System using that information.[20] Recovery of these systems helps to support the availability of information critical to the restoration of BES Cyber Systems. Accordingly, availability of information for medium and high impact BES Cyber Systems, and their associated EACMS and PACS, to aid in restoration is adequately addressed in the CIP Reliability Standards.

Other Reliability Standards and proposed revisions to Reliability Standards also provide for data availability. For instance, NERC developed the IRO and TOP Reliability Standards using availability of data as a guiding principle. In fact, one of the Reliability and Market Interface

---

18 NOI at P 12.

19 CIP-009-6, Requirement R1, Part 1.3.

20 CIP-009-6, Requirement R1, Part 1.4 and Requirement R2, Part 2.2

principles that the IRO and TOP Reliability Standards support is that "[i]nformation necessary for the planning and operation of interconnected bulk power systems shall be *made available* to those entities responsible for planning and operating the systems reliably."[21] [Emphasis added]

The NIST Framework includes redundancy of infrastructure or systems as a control that supports availability.[22] 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. The requirements for diversely routed data exchange infrastructure for Real-time Assessment and Real-time monitoring data within Control Centers align with suggested protections of availability in the NIST Framework to support data availability.

Reliability Standard EOP-008-2 helps support availability by requiring RCs to have backup Control Center facilities, or backup Control Center functionality for BAs and TOPs, in 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. As such, this redundancy helps support availability of not just the systems operating the Control Centers but also the information stored in those systems that is used to maintain and restore operations. As a result, EOP-008-2 helps to address the Commission's concern that loss of availability of certain information could impede the restoration or maintenance of BES reliability.

---

[21] *Standards Authorization Request Form for Modifications to TOP and IRO Standards at 4, available in Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards IRO-002-5 and TOP-001-4*, Exhibit F at 174, Docket No. RD17-4-000 (Mar. 6, 2017); *Standards Authorization Request Form* for Project 2014-03 Revisions to the TOP/IRO Reliability Standards at 6, available in *Petition of the North American Electric Reliability Corporation for Approval of Proposed Transmission Operations and Interconnection Reliability Operations and Coordination Reliability Standards*, Exhibit K at 483, Docket No. RM15-16-000 (Mar. 18, 2015).

[22] *See Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations* app. F-CP, at F-87 to F-88 (2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [hereinafter NIST 800-53].

Additionally, there are standards development projects in progress that will further strengthen protections for data availability. Project 2019-02 – BES Cyber System Information Access Management will include proposed revisions to CIP-011-2 and CIP-004-6 that will support availability of BES Cyber System Information. As stated in the Standard Authorization Request for that project, "[t]his initiative enhances BES reliability by creating… *higher availability* [emphasis added]… for entities to manage their BES Cyber System Information."[23] NERC provides updates to the Commission on the status of this project in Docket No. RD20-2-000.

PR.DS-6: While the Commission recognizes that CIP-013-1 includes requirements for integrity checking mechanisms, the Commission avers that these requirements do not apply to low impact BES Cyber Systems nor do they apply to information.[24] The ERO Enterprise agrees with the Commission that CIP-013-1 includes requirements for integrity checking mechanisms, but the ERO Enterprise also identified additional requirements, including future revisions, mapped to this Subcategory.

For low impact BES Cyber Systems, future standards revisions will address the integrity of software and firmware. 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. These revisions will help to further support

[23] NERC, *Standard Authorization Request – BES Cyber System Information Access Management*, 1, available at https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_SAR_BES%20Cyber%20System%20IAM%20Clean_112019.pdf.

[24] NOI at P 13.

the implementation of integrity checking mechanisms for assets containing low impact BES Cyber Systems.

Existing requirements in CIP-010-2 also map to this NIST Subcategory. CIP-010-2 addresses configuration change management, which in and of itself, is designed to focus on the integrity of applicable systems.[25] Specifically, CIP-010-2[26] 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-010-2, Requirement R2, Part 2.1 requires monitoring high impact BES Cyber Systems and their associated EACMS and PCAs for changes, including unauthorized changes. Future enforceable 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. As such, a number of the controls within CIP-010-2 and CIP-010-3 are designed to help support the integrity of BES Cyber Systems.

As for integrity of information addressed in the NIST Framework, CIP-011-2 Requirement R1, Part 1.2 maps to this NIST Framework control. Part 1.2 requires Responsible Entities to have procedures for protecting and securely handling BES Cyber System Information, including storage, transit, and use, as part of an implemented information protection program. These controls help to ensure information cannot be modified through unauthorized means, thereby supporting integrity of the BES Cyber System Information.

---

[25] NIST defines Configuration Management as "A collection of activities focused on establishing and maintaining the *integrity* [emphasis added] 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." NIST 800-53 app. B, at B-5.

[26] Reliability Standard CIP-010-3 includes the same Requirements R1 and R2.

While integrity checking mechanisms described above are important within NERC Reliability Standards, the ERO Enterprise also notes that some controls may not be appropriate for situations involving Real-time operations. Real-time systems rely on the availability of data and receiving data in a timely fashion. Certain integrity and confidentiality controls may slow down data needed in Real-time and cause issues. Therefore, the integrity checking mechanisms incorporated into NERC Reliability Standards must support Real-time operations.

b. Anomalies and Events

In the NIST Framework, the Anomalies and Events Category includes the objective that "[a]nomalous activity is detected and the potential impacts of events is understood."[27] Within the Anomalies and Events Category, there are two Subcategories identified by the Commission staff for further consideration as the subject of the NOI: (1) DE.AE-2 – Detected events are analyzed to understand attack targets and methods; and (2) DE.AE-4 – Impact of events is determined.[28] The following section describes how NERC Reliability Standards adequately address DE.AE-2 and DE.AE-4.

The Commission stated that the CIP-008-5 requirement to identify, classify, and respond to Cyber Security Incidents matches the Subcategories in the NIST framework to analyze detected events to understand attack targets and methods and to determine the impacts of events.[29] The Commission further stated, however, that this does not apply to low impact BES Cyber Systems.[30]

While the ERO Enterprise agrees that CIP-008-5 and CIP-008-6 address Subcategories DE.AE-2 and DE.AE-4, CIP-003-8 Requirement R2 maps to these Subcategories as well and is applicable to low impact BES Cyber Systems. Specifically, CIP-003-8 Requirement R2 requires a

27 NIST Framework 37-8.
28 NOI at P 16.
29 *Id.*
30 *Id.*

Responsible Entity to implement a cyber security plan that includes a section on Cyber Security Incident response for assets containing low impact BES Cyber Systems, as required by Section 4 of Attachment 1 that is incorporated by reference into Requirement R2. Moreover, part of that plan must include "identification, classification, and response to Cyber Security Incidents." These are the same controls the Commission cites as mapping to the NIST Subcategories for medium and high impact BES Cyber Systems. As such, these controls are adjusted for the risk that low impact BES Cyber Systems pose if compromised as a result of an event and map to the Anomalies and Events Category. As a result, the CIP Reliability Standards are adequate in addressing this control Category, commensurate with the risk posed by applicable systems.

c. Mitigation

In the NIST Framework, the Mitigation Category includes the objective that "[a]ctivities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident."[31] Within the Mitigation Category, there are three Subcategories identified by the Commission staff for further consideration as the subject of the NOI: (1) RS.MI-1 – Incidents are contained; (2) RS.MI-2 – Incidents are mitigated; and (3) RS.MI-3 – Newly identified vulnerabilities are mitigated or documented as accepted risks.[32] The following section describes how NERC Reliability Standards adequately address RS.MI-1, RS.MI-2, and RS.MI-3.

For all BES Cyber System impact levels, Responsible Entities are required to do more than only document plans. The Commission states that CIP-008-5 only requires Responsible Entities "document their cyber security incident response plans and provide evidence of incident response processes or procedures that address incident handling."[33] While CIP-008-5 Requirement R1, Part

---

31 NIST Framework 42.
32 NOI at P 18.
33 NOI at P 18.

1.4 requires Responsible Entities to document incident handling procedures in their Cyber Security Incident response plan, Requirement R2, Part 2.2 requires Responsible Entities to implement the plan, including incident handling procedures, when responding to a Reportable Cyber Security Incident.[34] As a result, Responsible Entities would contain and mitigate the effects of a Reportable Cyber Security Incident by activating the Cyber Security Incident response plan incident handling procedures. Likewise, Section 4.4 of Attachment 1 to Requirement R2 of CIP-003-8 requires Responsible Entities to include "Cyber Security Incident handling procedures" as part of their cyber security plans for assets containing low impact BES Cyber Systems. Moreover, CIP-003-8, Requirement R2 requires Responsible Entities to implement the plans. Based on these requirements, the ERO Enterprise determined that Subcategories RS.MI-1, RS.MI-2, and RS.MI-3 are adequately addressed by the CIP Reliability Standards at this time.

ii. Other Activities Align with NIST Framework

In addition to the Reliability Standards and standards development projects described in the previous Section I.A.i, the ERO Enterprise engages in other activities that incorporate the concepts from the NIST Framework, as described below.

Several of the Security Guidelines developed through the RSTC, and its predecessor the NERC Critical Infrastructure Protection Committee, rely on the NIST Framework to apply best

[34] In CIP-008-5, a Reportable Cyber Security Incident is defined as: "A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." In CIP-008-6, a Reportable Cyber Security Incident is defined as:

> A Cyber Security Incident that compromised or disrupted:
>
> - A BES Cyber System that performs one or more reliability tasks of a functional entity;
> - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
> - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.

practices in the context of BES cyber security.[35] For example, in 2019, the RSTC Supply Chain Working Group developed several guidelines regarding supply chain security that specifically reference NIST controls which are helpful to industry.

Furthermore, E-ISAC activities directly relate to the NIST Categories identified in the NOI. As it relates to the Anomalies and Events Category, the E-ISAC highlights critical vulnerabilities and patches that may require immediate patching based on reporting from the Cyber Security Risk Information Sharing Program ("CRISP"), a public-private partnership with the U.S. Department of Energy ("DOE") managed by the E-ISAC for NERC on behalf of participating utilities; U.S. Department of Homeland Security advisories; Federal Bureau of Investigation Pins; or DOE Analysis of Risks in the Energy Sector reports, giving these critical patches weighted importance over other more routine events. E-ISAC analysts add additional context specific to the electricity industry based on a variety of sources, and then communicate this through Cyber Bulletins, All Points Bulletins, or other methods 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.

In support of the Mitigation Category, 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. 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

[35] Security Guidelines are available at https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx.

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.

In further support of the Mitigation Category, the ERO Enterprise engages with industry groups to help address risk. 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.[36] In response, for example, 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.[37] These criteria and the associated questionnaire incorporate the applicable NERC standards and map to existing frameworks, such as the NIST Framework, in use by the vendor community.[38] 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 the Mitigation Category because entities are able to evaluate and identify the risk posed and develop appropriate mitigation prior to making a purchase. The ERO

[36] 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.

[37] 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* (2020), https://www.natf.net/docs/natf/documents/resources/supply-chain/energy-sector-supply-chain-risk-questionnaire---formatted.xlsx.

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

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.[39]

B. The ERO Enterprise recognizes the emerging threat of a coordinated cyber attack and continues to take action to minimize the risk.

The ERO Enterprise recognizes there is an evolving and emerging threat of a coordinated cyber attack against geographically distributed targets and takes action as necessary to mitigate the risk. The ERO Enterprise relies upon several tools in addition to standards development to address this risk, providing a defense-in-depth approach to risk mitigation. These tools include the following, among others: assessments, reports, and studies; alerts and lessons learned issuances; collaboration on risk prioritization with stakeholders; information sharing; and simulated training exercises. Each of these tools is discussed below.

In the NOI, the Commission highlighted two ERO Enterprise activities as identifying the risk of a coordinated cyber attack.[40] The first involved NERC's 2019 Supply Chain Risk Assessment that determined a coordinated cyber attack could impact BES reliability.[41] Based on this study, NERC determined to revise the CIP Reliability Standards to mitigate the risks posed by a coordinated attack through policies on supply chain risk management for assets containing low impact BES Cyber Systems. The second involved a Lessons Learned document that detailed a denial-of-service attack against multiple remote generation sites, which included recommendations that Responsible Entities adopt best practices.[42]

---

[39] 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).

[40] NOI at PP 24-26.

[41] *Id.* at P 25.

[42] *Id.* at P 26.

In addition, NERC provides assessments of risk and recommended mitigating actions in reports that highlight the emerging threat of a coordinated cyber attack. One such report, the State of Reliability Report, is issued on an annual basis. In the 2020 State of Reliability Report, NERC recognized the increasing risk of cyber security threats due to nation-state adversaries willing to exploit vulnerabilities that could result from the increasing digitization of the electric industry.[43] In this report, NERC recognized that so far the cyber security efforts of industry, the ERO Enterprise, the E-ISAC, and other government partners have been successful in supporting the reliable operation of the BES.[44] The report's recommendations include continuing to drive improvements in security posture through "technological hardening, growing a culture of security, and effective information exchange between entities, the E-ISAC, and trusted partner organizations."[45]

The NERC Alert process is another method that can be used to drive evaluation and mitigation of, protection against, and recovery from potential geographically distributed coordinated cyberattacks in a planned, coordinated manner. As part of its normal course of business, NERC often discovers, identifies, or is provided with information that is critical to ensuring the reliability of the Bulk-Power System in North America. In order to effectively disseminate this information, NERC issues email-based alerts designed to provide concise, actionable information to the electricity industry. As defined in its Rules of Procedure, 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.

---

[43] NERC, *2020 State of Reliability Report* (July 2020), 74, https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf.

[44] *Id.* 78.

[45] *Id.* 80.

2. Recommendation to Industry: Recommends specific action be taken by registered entities. A response from recipients, as defined in the alert, is required.

3. Essential Action: Identifies actions deemed to be "essential" to Bulk-Power System 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 ERO Enterprise also collaborates on studies to understand how Reliability Standards requirements address risk. For example, the ERO Enterprise is assessing the efficacy of electronic access controls 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.[46] The results of this study will provide input on how effective these controls are at protecting low impact BES Cyber Systems, including from the risk of a coordinated cyber attack.

The ERO Enterprise also recognizes collaboration with industry as essential to identifying and mitigating risk. One forum for monitoring emerging risks to the BES is the Reliability Issues Steering Committee ("RISC"). The RISC is an advisory committee to the NERC Board of Trustees and provides key insights, priorities, and high-level leadership for issues of strategic importance to BES reliability. In addition, the RISC supports development of solutions to address these emerging reliability issues. The guidance provided by the RISC helps the ERO Enterprise and the industry to effectively focus resources on the critical issues to improve the reliability of the BES. In the 2019 ERO Reliability Risk Priorities Report, the RISC identified coordinated cyber attacks as part of its risk profile in security risks.[47] The RISC also included recommended actions that help

---

[46] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 163 FERC ¶ 61,032 at P 30 (2018).

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

to address the risk of a coordinated cyber attack, which focused on increased information sharing and enhanced analysis of the emerging risks.[48] The recommendations did not include revisions to the CIP Reliability Standards at this time.

Furthermore, this broad collaboration with industry is particularly important in mitigating the risk of a coordinated cyber attack across a geographic area given the unique nature of that threat. The NATF activities mentioned in Section I.A above help to support identification of supply chain risks that may lead to a coordinated cyber attack. These efforts go beyond providing benefits for NATF members; NATF collaborates with other industry trade associations, suppliers, third-party assessors, and solution providers. To that end, NERC and NATF have planned regional webinars and workshops to support entities in their supply chain risk mitigation efforts. This collaboration helps entities to better identify a risk that could impact several entities, such as a coordinated cyber attack, and helps to develop appropriate mitigation solutions.

In light of the evolving nature of threats to the Bulk-Power System, the ERO Enterprise also adjusts its business operations as needed to appropriately assess risk. For example, NERC has recently formed the Bulk-Power System 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 Bulk-Power System continues to evolve in terms of its resource mix and technologies being utilized in operational technology, information technology, and industrial controls systems, it is critical for security considerations to be at the forefront of engineering and business decisions. Planners will need to consider new threat vectors, such as a coordinated cyber attack, that could impact reliable operation of the Bulk-Power System in the planning horizon. Bulk-Power System

[48] *Id.* 23.

operators should be equipped with tools and capabilities to quickly respond and adapt to possible security threats. Bulk-Power System physical protection and controls designs should minimize the extent of cyber threats while seeking operational advancements using new technologies. The Bulk-Power System 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.

Information sharing in real-time provides a key component in mitigating risk, particularly for a coordinated cyber attack across a large geographic area that may involve different entities. The E-ISAC informs industry of potential threats to the grid and would be able to help industry mitigate potential geographically distributed coordinated cyber attacks. This is contingent on the industry, as a whole, alerting the E-ISAC to anomalies or potential cyber attacks occurring, as well as information sharing by Federal departments and agencies. Industry partners communicate well with the E-ISAC for even minimal issues, such as phishing alerts, to make others aware of potential threats. These alerts are then made available to all industry partners to ensure the security of the Bulk-Power System.

Additionally, E-ISAC coordinates, in participation with the DOE and the Pacific Northwest National Laboratory ("PNNL"), in CRISP. CRISP is a data sharing and analysis program that 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, NERC and the E-ISAC test the ability of the grid to respond to coordinated cyber and physical attacks in the biennial Grid Security Exercise ("GridEx"). The focus of GridEx is continent-wide, with coordinated cyber and physical attack 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. In particular, GridEx enables Bulk-Power System and distribution utilities to exercise and drill their response and recovery plans, including across a geographically distributed coordinated cyber and physical attack. The below results from a survey taken by GridEx V participants in 2017 demonstrates the effectiveness of the exercise and the value it provides to those involved:

- 96% of respondents felt GridEx V met their expectations with 65% indicating "very well" (up from 42% in GridEx IV); and
- 97% of respondents felt GridEx V was planned and managed to meet their needs with 64% indicating "very well" (up from 38% in GridEx IV).[49]

NERC and the E-ISAC are committed to continue enhancing the GridEx program to meet the challenges posed by the ever-evolving threat environment.

Finally, new Reliability Standard requirements coming into effect will help to identify and contain risks before they could become a bigger coordinated cyber attack. Reliability Standard CIP-008-6, which will become effective in the United States on January 1, 2021, broadens the mandatory reporting of Cyber Security Incidents to include compromises or attempts to compromise BES Cyber Systems or their associated Electronic Security Perimeters or EACMS. E-ISAC will receive these expanded reports, and to facilitate implementation of the new requirements, E-ISAC has been working with industry to refine what sort of incidents could be considered attempts to compromise.

[49] E-ISAC, *GridEx V Grid Security Exercise: Lessons Learned Report* (Mar. 2020) at viii, https://www.nerc.com/pa/CI/CIPOutreach/GridEX/TLP%20WHITE%20GridEx%20V%20Lessons%20Learned%20MAR20.pdf.

Should NERC identify additional risks and potential procedures to mitigate them, such as Reliability Standards revisions, NERC would recommend them and take action. Again, it is a defense-in-depth approach that is employed to combat cyber security risks. Reliability Standards are one of a number of tools used to mitigate cyber security risks, including the risk of a coordinated attack. If the ERO Enterprise identifies a risk requiring enhanced mitigation measures, it will address the issue through a combination of standards development activity, if necessary, and its other reliability tools, including security guidelines, increased information sharing, training exercises, and alerts.

As described above, the ERO Enterprise is active in identifying and addressing risks posed by coordinated cyber attack. Nonetheless, the ERO Enterprise is interested in reviewing the comments in this proceeding on areas for improvement, if any. However, the ERO Enterprise cautions that if additional controls are recommended, the application of controls must be risk-based, consistent with the intent behind CIP-002-5.1a. CIP-002-5.1a uses the bright-line criteria to determine impact and to identify and categorize high and medium BES Cyber Systems and assets that contain low impact BES Cyber Systems. Low impact BES Cyber Systems have different protections commensurate with the risk posed to the BES so that entities can focus resources on higher risk assets. As such, the ERO Enterprise respectfully requests the Commission consider resource allocation. This consideration must include allocating resources to the highest risk areas.

II. CONCLUSION

As discussed above, the ERO Enterprise appreciates the opportunity to address the Commission's concerns. The ERO Enterprise consistently looks to the NIST Framework to inform all its cyber security activities, including standards development, standards implementation, and non-mandatory activities that support BES reliability. The ERO Enterprise also recognizes there are evolving and emerging threats, such as the potential risk for a coordinated cyber attack on geographically distributed targets. The ERO Enterprise assesses the appropriate course of action and takes action as necessary to mitigate the risk. As such, the ERO Enterprise respectfully requests the Commission consider all the activities the ERO Enterprise performs when contemplating any next steps.

Respectfully submitted,

/s/ Marisa Hecht

Shamai Elstein
Assistant General Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
shamai.elstein@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: August 24, 2020