NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

December 21, 2020

VIA ELECTRONIC FILING

Mr. Neil Cunningham
Director of Climate Change and Energy Branch
Department of Sustainable Development
1200-155 Carlton Street
Winnipeg MB R3C 3H8

RE: *North American Electric Reliability Corporation*

Dear Mr. Cunningham:

The North American Electric Reliability Corporation ("NERC") hereby submits Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 Addressing Supply Chain Cybersecurity Risk Management. NERC requests, to the extent necessary, a waiver of any applicable filing requirements with respect to this filing.

NERC understands that the Province of Manitoba enacted on April 1, 2012, the Reliability Standards Regulation, which was implemented through an Order of Council. It is NERC's understanding that the Reliability Standards Regulation makes compliance with the NERC reliability standards a legal requirement in Manitoba and adopted the NERC Reliability Standards listed in Schedule 1 of the Regulation for implementation in Manitoba. The Regulation further provides that a reliability standard made by NERC that is listed in Schedule 1 is adopted as a reliability standard for Manitoba.

NERC requests that Manitoba take all necessary action to include Proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 as set forth in the filing in Schedule 1 of the Reliability Standards Regulation, so that they may be adopted as reliability standards for Manitoba.

Please contact the undersigned if you have any questions concerning this filing.

Sincerely,

/s/ Lauren Perotti

Lauren Perotti
Senior Counsel for the North American Electric Reliability Corporation

1325 G Street NW Suite 600
Washington, DC 20005
202-400-3000 | www.nerc.com

BEFORE THE
PROVINCE OF MANITOBA

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARDS CIP-013-2, CIP-005-7, AND CIP-010-4 ADDRESSING SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT

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

Counsel for the North American Electric Reliability Corporation

December 21, 2020

TABLE OF CONTENTS

BEFORE THE
PROVINCE OF MANITOBA

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARDS CIP-013-2, CIP-005-7, AND CIP-010-4 ADDRESSING SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT

The North American Electric Reliability Corporation ("NERC") hereby submits proposed Reliability Standards CIP-013-2 – Cyber Security – Supply Chain Risk Management, CIP-005-7 – Cyber Security – Electronic Security Perimeter(s), and CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments. The proposed Reliability Standards improve the reliability of the Bulk Electric System ("BES") and address the Federal Energy Regulatory Commission's ("FERC") directive from Order No. 850 [1] to develop modifications to include Electronic Access Control or Monitoring Systems ("EACMS") [2] associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards. In addition, the proposed Reliability Standards address the NERC recommendation to address Physical Access Control Systems ("PACS") that provide physical access control to high and medium impact BES Cyber Systems.[3] The proposed Reliability

[1] *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018) [hereinafter Order No. 850].

[2] 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.

[3] While the recommendation excluded the alarming and logging functions of PACS, the standard drafting team determined to include these functions of PACS in applicability. NERC, *NERC Cyber Security Supply Chain Risks: Staff Report and Recommended Actions*, FERC Docket No. RM17-13-000 (2019) [hereinafter NERC Supply Chain Report], at https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Supply%20Chain%20Report%20Filing.pdf.

Standards, provided in Exhibit A hereto, are just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

NERC also provides notice of: (1) the associated Implementation Plan (Exhibit B); the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibit G); and the retirement of currently-effective Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3.

This filing presents the technical basis and purpose of the proposed Reliability Standards, a summary of the development history (Exhibit H), and a demonstration that the proposed Reliability Standards meet the Reliability Standards criteria (Exhibit C). The NERC Board of Trustees adopted the proposed Reliability Standards on November 5, 2020.

I. SUMMARY

In Order No. 850, FERC approved Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 (the "Supply Chain Standards"). The Supply Chain Standards, which were developed in response to FERC Order No. 829,[4] address cybersecurity risks associated with the supply chain for BES Cyber Systems. In approving the Supply Chain Standards, FERC found that they addressed the following four objectives from Order No. 829: (1) software integrity and authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls.[5] FERC further directed NERC to modify the Supply Chain Standards to include EACMS as applicable systems and file the modifications within 24 months of the effective date of Order No. 850.[6] Finally, FERC accepted NERC's commitment to study certain categories of assets not currently the subject of the Supply Chain Standards,

[4] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016) [hereinafter Order No. 829].

[5] Order No. 850 at P 28. These four objectives were the subject of directives from Order No. 829.

[6] Order No. 850 at PP 30, 52.

including PACS.[7] On May 28, 2019, NERC filed a report detailing NERC's assessment of supply chain risks as well as any recommended actions.[8] One such recommended action included modifications to the applicability of the Supply Chain Standards to include PACS.[9]

Consistent with Order No. 850 and the NERC Supply Chain Report, proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 (proposed "Supply Chain Standards") broaden supply chain risk management requirements to include EACMS and PACS as applicable systems. EACMS are devices that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter ("ESP") or BES Cyber Systems. As such, EACMS (e.g., firewalls or security information event management systems, among others) control or monitor electronic access to some of the most critical systems operating the BES. PACS are devices that control, alert, or log access to the Physical Security Perimeter ("PSP").[10] These devices help to manage physical access to defined areas that physically contain medium and high impact BES Cyber Systems. Similar to EACMS, PACS manage physical access to some of the most critical systems operating the BES. As such, including both EACMS and PACS as applicable systems in the Supply Chain Standards further enhances the reliability of the BES. The proposed Reliability Standards maintain the security objectives supported in the original version of the Supply Chain Standards while expanding protections for these additional applicable systems.

---

7 Order No. 850 at P 31.

8 NERC Supply Chain Report.

9 *Id.* at pp. 15-16.

10 This does not include locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

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

Howard Gugel
Vice President, Engineering and Standards
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
howard.gugel@nerc.net

III. BACKGROUND

A. NERC Reliability Standards Development Procedure

The proposed Reliability Standards were developed in an open and fair manner and in accordance with the Reliability Standard development process. NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[11] NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain criteria for approving Reliability Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders. Further, a vote of stakeholders and adoption by the NERC Board of Trustees is

[11] The NERC Rules of Procedure are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

required before NERC submits the Reliability Standard to the applicable governmental authorities for approval.

B. Order No. 850 Directive

The Supply Chain Standards, submitted on October 2, 2017,[12] were developed in response to directives in FERC Order No. 829. In Order No. 829, FERC directed NERC "to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with [BES] operations."[13]

In Order No. 850,[14] FERC approved supply chain risk management Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 and directed additional modifications. Specifically, FERC directed NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Standards.[15] FERC declined to direct further detail, determining the following:

> [W]e leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risk. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.[16]

FERC further noted that the standard drafting team could determine that a subset of EACMS may be appropriate for applicability of the supply chain risk management requirements, citing the EACMS functions identified in Order No. 848.[17] FERC directed NERC to file the modifications

---

[12] *Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management,* Oct. 2, 2017.

[13] Order No. 829 at P 2 (internal citations omitted).

[14] Order No. 850.

[15] *Id.*at PP 30, 51.

[16] *Id.* at P 51.

[17] *Id.* at P 55 (citing *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033 (2018)).

within 24 months of the effective date of Order No. 850.[18] In addition, FERC accepted NERC's commitment to study certain categories of assets not currently subject to the Supply Chain Standards and directed NERC to file the final report, discussed below, with FERC upon its completion.[19]

C. NERC Supply Chain Report

In adopting the Supply Chain Standards in August 2017, the NERC Board of Trustees issued resolutions[20] directing NERC to continue working with industry and vendors on supply chain issues, including further study of supply chain risks, among other activities. In carrying out the resolution to further study supply chain risk, NERC evaluated supply chain risks associated with certain categories of assets not subject to the Supply Chain Standards submitted on October 2, 2017 and approved in FERC Order No. 850. Based on this evaluation, NERC developed a report that included recommended actions to address those supply chain risks.[21] That report recommended the following standards modifications: (1) revise the Supply Chain Standards to address EACMS that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems; and (2) revise the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems.[22] NERC filed the NERC Supply Chain Report with FERC on May 28, 2019.[23]

---

18 The effective date of Order No. 850 in the U.S. was December 26, 2018.

19 Order No. 850 at P 31.

20 The NERC Board of Trustees resolutions are available at https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

21 NERC Supply Chain Report.

22 *Id.* at pp. 9-11 and 15-16.

23 *Id.*

D. Development of the Proposed Reliability Standards

As further described in Exhibit H hereto, NERC initiated a Reliability Standard development project, Project 2019-03 Cyber Security Supply Chain Risks ("Project 2019-03"), and appointed a standard drafting team (Exhibit I) to address the Order No. 850 directive and the NERC Supply Chain Report recommendations. On January 27, 2020, NERC posted the initial drafts of proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 for a 45-day comment period and ballot. The initial ballot did not receive the requisite approval from the registered ballot body ("RBB"). After considering comments to the initial drafts, NERC posted second drafts of the proposed Reliability Standards for another 45-day comment period and ballot on May 5, 2020. The second drafts did not receive the requisite approval from the RBB. On July 28, 2020, NERC posted the third drafts of the proposed Reliability Standards after considering comments on the second drafts. The third drafts received the requisite approval from the RBB with an affirmative vote of 80.78 percent at 79.93 quorum. NERC conducted a 10-day final ballot for the proposed Reliability Standards, which received an affirmative vote of 76.76 percent at 83.56 quorum. The NERC Board of Trustees adopted the proposed Reliability Standards on November 5, 2020.

IV. JUSTIFICATION

As discussed below and in Exhibit C, the proposed Reliability Standards enhance reliability by expanding the scope of protected equipment to include EACMS and PACS, thereby addressing FERC's directive in Order No. 850 and the NERC Supply Chain Report recommendations, and are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The proposed revisions incorporate EACMS and PACS as applicable systems in the Supply Chain Standards through language that accounts for the unique role played by these systems, particularly by EACMS. The following section discusses the revisions to the standards:

- the revised Requirement R1 in proposed Reliability Standard CIP-013-2 (Subsection A)
- the new Requirement R3 in proposed Reliability Standard CIP-005-7 (Subsection B); and
- the revised applicability in proposed Reliability Standard CIP-010-4 (Subsection C).

This section concludes with a discussion of the enforceability of the proposed Reliability Standards (Subsection D).

A. Proposed Reliability Standard CIP-013-2

Proposed Reliability Standard CIP-013-2 requires Responsible Entities to consider and address cyber security risks from vendor products or services during planning for the procurement of BES Cyber Systems as well as EACMS and PACS. Proposed Reliability Standard CIP-013-2 includes three requirements: (1) Requirement R1 requires a Responsible Entity to develop documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and includes requirement parts detailing the processes to include in the plan; (2) Requirement R2 requires Responsible Entities to implement the plan(s); and (3) Requirement R3 requires review and CIP Senior Manager, or delegate, approval of the plan(s) at least once every 15 calendar months.

Proposed Reliability Standard CIP-013-2 only includes modifications to Requirement R1, although the entire standard applies to EACMS and PACS. The modifications are shown in blackline below:

> **R1.** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems **and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)**. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
>
> **1.1.** One or more process(es) used in planning for the procurement of BES Cyber Systems **and their associated EACMS and PACS** to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and

installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems**, and their associated EACMS and PACS,** that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System **and their associated EACMS and PACS**; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated ~~Interactive Remote Access, and (ii) system-to-system~~ remote access ~~with a vendor(s)~~.

The revisions to Requirement R1 require Responsible Entities to add EACMS and PACS associated with medium and high impact BES Cyber Systems to documented supply chain cyber security risk management plans. These requirements address risks during the planning stage when procuring BES Cyber Systems, EACMS, and PACS. The revisions to Requirement R1 now require that Responsible Entities: (1) adequately consider security risks when planning for EACMS and PACS associated with high and medium impact BES Cyber Systems (Part 1.1); and (2) address relevant security concepts in future contracts for EACMS and PACS associated with high and medium impact BES Cyber Systems (Part 1.2).

Additionally, revised Part 1.2.6 clarifies requirements surrounding remote access to accommodate applicability to EACMS and PACS by removing the term Interactive Remote Access and the phrase "system-to-system." This revision helps to coordinate with language in new Requirement R3 in proposed Reliability Standard CIP-005-7, as more fully described in Section IV.B. below, and continues to work in tandem with proposed CIP-005-7, Requirement R2, Parts 2.4 and 2.5. The revised requirement still achieves the objective of providing for vendor remote access protections as directed in Order No. 829.[24]

B. Proposed Reliability Standard CIP-005-7

Proposed Reliability Standard CIP-005-7 includes requirement parts that address supply chain risk management in the operational phase. The existing Parts 2.4 and 2.5 include remote access controls for high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. Proposed new Requirement R3, which includes new Parts 3.1 and 3.2, addresses remote access controls for EACMS and PACS associated with high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. Proposed Requirement R3 reads as follows:

> **R3.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.

Within Requirement R3, CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS includes two new requirement parts. Proposed Parts 3.1 and 3.2 apply to EACMS and PACS associated with: (1) high impact BES Cyber Systems; and (2) medium impact

[24] Order No. 829 at P 51.

BES Cyber Systems with External Routable Connectivity. Proposed Parts 3.1 and 3.2 provide as follows:

> **3.1** Have one or more method(s) to determine authenticated vendor-initiated remote connections.
>
> **3.2** Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.

These new requirement parts work in tandem with Requirement R1, Part 1.2.6 of proposed Reliability Standard CIP-013-2 (discussed in Section IV.A above) to address vendor remote access and are similar to CIP-005-7, Requirement R2, Parts 2.4 and 2.5, which address remote access controls in the operational phase for medium and high impact BES Cyber Systems. However, based on the functions EACMS perform, there are some key distinctions in Parts 3.1 and 3.2 compared to Parts 2.4 and 2.5, as described below.

EACMS perform several monitoring and managing functions, including acting as an Intermediate System. Under Requirement R2, Part 2.1, Responsible Entities must use an Intermediate System, which is a type of EACMS, for Interactive Remote Access to a high impact BES Cyber System and a medium impact BES Cyber System with External Routable Connectivity. In performing this function, the EACMS is controlling the remote access to the BES Cyber System. As such, those vendors seeking to use Interactive Remote Access with an applicable BES Cyber System would first need to be authorized by the EACMS – in this case, an Intermediate System. In performing this role, the EACMS appropriately would deny access to a vendor that is not authorized. The standard drafting team did not want this normal function of an EACMS to be considered a "session" for purposes of applying the supply chain risk management protections simply because the vendor interacted with the EACMS but did not gain access to the BES Cyber System. Accordingly, the term "connection" describes when an authorized vendor is granted

access by the EACMS. Parts 3.1 and 3.2 use the terms "connection" instead of "session," which is used in Parts 2.4 and 2.5.

Likewise, Parts 3.1 and 3.2 do not use the terms "Interactive Remote Access" or "system-to-system remote access" (as used in Parts 2.4 and 2.5) because the standard drafting team determined the term "access" could be ambiguous when applied to EACMS. Based on comments received, the standard drafting team identified that "access" could be interpreted to include the Intermediate System function scenario described above, where a vendor interacts with an EACMS but is denied access to the BES Cyber System due to lack of authorization. As a result, the standard drafting team did not carry over the references to "Interactive Remote Access" and "system-to-system remote access" from Parts 2.4 and 2.5 in CIP-005-7, Requirement R3, Parts 3.1 and 3.2.

Finally, the term "authenticated" was used to describe access that has already been established by a user. As an EACMS can perform an authenticating function, the standard drafting team again determined this better described those connections that had already been established (subject to Requirement R3) versus those connections that were trying to be established (not subject to Requirement R3). Finally, the standard drafting team chose to use "terminate" combined with "control the ability to reconnect" instead of "disable" (which is used in Part 2.5) in Part 3.2 because it more granularly described the methods entities should employ when managing access to EACMS.

C. Proposed Reliability Standard CIP-010-4

Proposed Reliability Standard CIP-010-4 includes revisions to the applicability in Requirement R1, Part 1.6. The proposed revisions expand applicability to: (1) EACMS associated with high and medium impact BES Cyber Systems; and (2) PACS associated with high and medium impact BES Cyber Systems. As such, Requirement R1, Part 1.6 of proposed Reliability Standard CIP-010-4, whose requirement language remains unchanged from CIP-010-3, includes

the following as applicable to high and medium impact BES Cyber Systems and their associated EACMS and PACS:

> **1.6** Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:
>
> 1.6.1. Verify the identity of the software source; and
>
> 1.6.2. Verify the integrity of the software obtained from the software source.

In its filing of CIP-013-1, CIP-005-6, and CIP-010-3, NERC explained that:

> Essentially, Part 1.6 provides that prior to installing software that changes the established baseline configuration for (1) operating system(s) (including version) or firmware where no independent operating system exists (Part 1.1.1), (2) any commercially available or open-source application software (including version) intentionally installed (Part 1.1.2), or (3) any custom software installed (Part 1.1.3), Responsible Entities must verify the identity of the software source and the integrity of the software obtained by the software sources, when methods are available to do so…. These steps, as FERC stated in Order No. 829, help "reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System."[25]

As revised, the standard will now help reduce the risk of an attacker exploiting this process for EACMS and PACS by requiring Responsible Entities to apply these protections to EACMS and PACS.

Similar to Parts 2.4 and 2.5 and Requirement R3 of proposed CIP-005-7, proposed CIP-010-4, Requirement R1, Part 1.6 complements the procurement requirements in CIP-013-2 by requiring Responsible Entities to verify software integrity and authenticity for EACMS and PACS in the operational phase.

---

[25] *Notice of Filing of the North American Electric Reliability Corporation of Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, Oct. 2, 2017, p. 31-32 (citing FERC Order No. 829 at P 49).

D. Other Modifications

The proposed Reliability Standards also contain a number of minor modifications to align the standards with revisions to other standards or initiatives in other areas. These changes are shown in redline in Exhibit A and are summarized below.

The Interchange Coordinator or Interchange Authority is removed from the Applicability section of proposed Reliability Standards CIP-005-7 and CIP-010-4. This revision is consistent with changes to the NERC Compliance Registry under the risk-based registration initiative.[26]

Additionally, the proposed Reliability Standards include other minor modifications to the non-enforceable sections of the standard.

E. Enforceability of Proposed Reliability Standards

The proposed Reliability Standards also include measures that support each requirement by clearly identifying what is required and how the ERO will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party. Additionally, the proposed Reliability Standards include VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standards. The VRFs and VSLs for the proposed Reliability Standards comport with NERC and FERC guidelines related to their assignment. Exhibit G provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

[26] *Notice of Filing of the North American Electric Reliability Corporation of Risk-Based Registration Initiative Rules of Procedure Revisions*, Jan. 6, 2015 (notice of removal of the Purchasing Selling Entity and Interchange Authority/Coordinator from the NERC Compliance Registry).

V. EFFECTIVE DATE

The proposed Reliability Standards are set forth in the proposed Implementation Plan, provided in Exhibit B hereto. The proposed Implementation Plan provides that, where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority. Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction. The 18-month implementation period is designed to afford Responsible Entities sufficient time to develop and implement their supply chain cybersecurity risk management plans incorporating EACMS and PACS associated with high and medium BES Cyber Systems according to proposed Reliability Standard CIP-013-2, implement the new requirement in proposed Reliability Standard CIP-005-7 for EACMS and PACS associated with high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity, and implement the controls in proposed Reliability Standard CIP-010-4, Requirement R1, Part 1.6 for EACMS and PACS.

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, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: December 21, 2020

EXHIBITS A - B and D - I

EXHIBIT C

Reliability Standards Criteria

The discussion below explains how the proposed Reliability Standards meet or exceed the Reliability Standards criteria.

1. **Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.**

The proposed Reliability Standards enhance the cybersecurity posture of the electric industry by broadening the applicable systems to which the protections in the Supply Chain Standards apply. Consistent with the directive in FERC Order No. 850, the supply chain requirements in CIP-013-2, CIP-005-7, and CIP-010-4 apply to Electronic Access Control or Monitoring Systems ("EACMS"). Moreover, consistent with the recommendations in the NERC Supply Chain Report, the supply chain requirements also apply to Physical Access Control Systems ("PACS"). As such, the proposed Reliability Standards enhance the reliability of the BES by addressing supply chain risk management for EACMS and PACS.

2. **Proposed Reliability Standards must be applicable only to users, owners and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.**

The proposed Reliability Standards are clear and unambiguous as to what is required and who is required to comply. The proposed Reliability Standards apply to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed Reliability Standards clearly articulate the actions that such entities must take to comply with the standard.

3. **A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.**

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for the proposed Reliability Standards comport with NERC and FERC guidelines related to their assignment, as discussed further in Exhibit D. The assignment of the severity level for each VSL is consistent with the corresponding requirement. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standards include clear and understandable consequences.

4. **A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner.**

The proposed Reliability Standards contain measures that support the requirements by clearly identifying what is required to demonstrate compliance. These measures help provide clarity regarding the manner in which the requirements will be enforced and help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party. The measures are substantively unchanged from the currently effective version of the standard.

5. **Proposed Reliability Standards should achieve a reliability goal effectively and efficiently — but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.**

The proposed Reliability Standards achieve the reliability goals effectively and efficiently. The proposed Reliability Standards clearly articulate the security objective that applicable entities must meet and provide entities the flexibility to tailor their processes and plans required under the standard to best suit the needs of their organization.

6. **Proposed Reliability Standards cannot be "lowest common denominator," *i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.**

The proposed Reliability Standards do not reflect a "lowest common denominator" approach. The proposed Reliability Standards broaden the applicable systems to which the Supply Chain Standards apply. Furthermore, the proposed Reliability Standards go beyond the FERC Order No. 850 directive with minimal to no use of subsets of EACMS and PACS.

7. **Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.**

The proposed Reliability Standards apply throughout North America and do not favor one geographic area or regional model.

8. **Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.**

The proposed Reliability Standards have no undue negative impact on competition. The proposed Reliability Standards require the same performance by each of the applicable Functional Entities. The proposed Reliability Standards do not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

9. **The implementation time for the proposed Reliability Standard is reasonable.**

The proposed implementation period for the proposed Reliability Standards is just and reasonable and appropriately balances the urgency in the need to implement the standard against

the reasonableness of the time allowed for those who must apply appropriate protections on EACMS and PACS.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Reliability Standard development process.

The proposed Reliability Standards were developed in accordance with NERC's ANSI-accredited processes for developing and approving Reliability Standards. Exhibit E includes a summary of the development proceedings and details the processes followed to develop the proposed Reliability Standards. These processes included, among other things, comment and ballot periods. Additionally, all meetings of the drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum, and the last additional ballot and final ballot exceeded the required ballot pool approval levels.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.

NERC has identified no competing public interests regarding the r proposed Reliability Standards. No comments were received that indicated the proposed Reliability Standards conflict with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.

No other negative factors relevant to whether the proposed Reliability Standards are just and reasonable were identified.