NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

September 23, 2021

VIA ELECTRONIC FILING

Ms. Christine E. Long
Registrar & Board Secretary
Ontario Energy Board
27th Floor 2300 Yonge Street
Toronto, ON M4P 1E4

Re: *North American Electric Reliability Corporation*

Dear Ms. Long:

The North American Electric Reliability Corporation ("NERC") hereby submits Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards CIP-004-7 and CIP-011-3 Addressing Bulk Electric System Cyber System Information Access Management. NERC requests, to the extent necessary, a waiver of any applicable filing requirements with respect to this filing.

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

ONTARIO ENERGY BOARD
OF THE PROVINCE OF ONTARIO

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION)
)

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARDS CIP-004-7 AND CIP-011-3 ADDRESSING BULK ELECTRIC SYSTEM CYBER SYSTEM INFORMATION ACCESS 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

September 23, 2021

TABLE OF CONTENTS

ONTARIO ENERGY BOARD
OF THE PROVINCE OF ONTARIO

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION)
)

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARDS CIP-004-7 AND CIP-011-3 ADDRESSING BULK ELECTRIC SYSTEM CYBER SYSTEM INFORMATION ACCESS MANAGEMENT

The North American Electric Reliability Corporation ("NERC") hereby submits for approval proposed Reliability Standards CIP-004-7 – Cyber Security – Personnel & Training and CIP-011-3 – Cyber Security – Information Protection. The proposed Reliability Standards improve the reliability of the Bulk Electric System ("BES") by clarifying the protections required regarding use of third-party solutions for BES Cyber System Information ("BCSI"). The proposed Reliability Standards, provided in Exhibit A hereto, are just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

NERC also requests approval of: 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-004-6 and CIP-011-2.

This petition 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 August 12, 2021.

I. SUMMARY

The suite of Critical Infrastructure Protection ("CIP") Reliability Standards require protections around BES Cyber Systems, the most critical cyber devices on the electric grid. As

defined in the NERC Glossary of Terms used in Reliability Standards ("NERC Glossary"), BCSI is "[i]nformation about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System."[1] Given the importance of BCSI, Responsible Entities must control access to this information. In currently effective Reliability Standards CIP-004-6 and CIP-011-2, Responsible Entities do this by managing access to the "designated storage location" of BCSI, such as an electronic document or physical file room. However, as technology has evolved, third-party services, such as cloud services, have become a viable and safe option for storing BCSI. The protections available for Responsible Entities to secure information in the cloud, for example, depend less on the actual storage location of the information and more on file-level rights and permissions. As a result, the revisions in proposed Reliability Standards CIP-004-7 and CIP-011-3 would allow Responsible Entities to leverage these protections within their control for third-party data storage and analysis systems.

To that end, proposed CIP-004-7, which pertains to personnel and training, includes the following modifications:

- Removes references to "designated storage locations" of BCSI;
- Adds Requirement R6 regarding an access management program to authorize, verify, and revoke provisioned access to BCSI; and
- Other minor clarifications to update the standard.

[1] The rest of the definition also states:
BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
The NERC Glossary is available at https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

Proposed Reliability Standard CIP-011-3, which pertains to information protection, includes the following modifications:

- Clarifies requirements regarding protecting and securely handling BCSI; and
- Other minor clarifications to update the standard.

The proposed Reliability Standards maintain the security objectives supported in previous versions while providing flexibility for Responsible Entities to leverage third-party data storage and analysis systems. As such, the proposed Reliability Standards are just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

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.[2] 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 required before NERC submits the Reliability Standard to the applicable governmental authorities.

B. Standard Drafting Team Schedule Directive

In an order issued on February 20, 2020, the Federal Energy Regulatory Commission ("FERC") directed NERC to submit an informational filing outlining the project schedules for Projects 2016-02[3] and 2019-02.[4] Pursuant to paragraph 5 of the Schedules Order,[5] FERC stated that these schedules should include the status of the projects, interim target dates, and the anticipated filing date for new or modified Reliability Standards. In addition, FERC directed NERC to file quarterly informational status updates, beginning in June 2020, until NERC files new or modified standards with FERC.[6]

NERC provided the initial informational filing regarding the schedules on March 19, 2020[7] and four additional quarterly informational filings with updated schedules on June 19, 2020,[8]

---

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

[3] Project 2016-02 – Modifications to CIP Standards focuses on modifications to the suite of CIP Reliability Standards to incorporate applicable protections for virtualized environments.

[4] *N. Am. Elec. Reliability Corp.*, "Order Directing Informational Filings Regarding NERC Standard Drafting Projects," 170 FERC ¶ 61,109 (Feb. 20, 2020) [hereinafter Schedules Order].

[5] *Id.*

[6] *Id.*

[7] NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (March 19, 2020).

[8] NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (June 19, 2020).

September 17, 2020,[9] December 15, 2020,[10] March 15, 2021,[11] and June 15, 2021.[12] NERC also provided a supplemental informational filing on November 13, 2020.[13] With this filing, NERC concludes the updates to FERC for Project 2019-02.[14]

C. Development of the Proposed Reliability Standards

As further described in Exhibit H hereto, NERC initiated a Reliability Standard development project, Project 2019-02 BES Cyber System Information Access Management ("Project 2019-02"), and appointed a standard drafting team (Exhibit I) to develop the revisions. This project was initiated due to the work of an informal team, in collaboration with the NERC Compliance Input Working Group,[15] to review the use of encryption on BCSI and its impact on compliance with NERC Reliability Standards.

On December 20, 2019, NERC posted the initial drafts of proposed Reliability Standards CIP-004-7 and CIP-011-3 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 August 6, 2020. The second drafts did not receive the requisite approval from the RBB. On March 25, 2021, NERC posted the third drafts of the proposed

---

[9] NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (September 17, 2020).

[10] NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (December 15, 2020).

[11] NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (March 15, 2021).

[12] NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (June 15, 2021).

[13] NERC, *Supplemental Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (November 13, 2020).

[14] As directed, NERC will continue to file updates to FERC on Project 2016-02 until those revisions are filed in a petition for approval to FERC.

[15] The Compliance Input Working Group was a subgroup of the now-disbanded NERC Critical Infrastructure Protection Committee, a stakeholder technical committee.

Reliability Standards after considering comments on the second drafts. The third drafts received the requisite approval from the RBB with an affirmative vote of 83.75 percent at 84.31 quorum for proposed CIP-004-7 and an affirmative vote of 81.39 percent at 84.62 quorum for proposed CIP-011-3.[16] On June 2, 2021, NERC conducted a 10-day final ballot for the proposed Reliability Standards, which received an affirmative vote of 85.8 percent at 86.5 quorum for proposed CIP-004-7 and an affirmative vote of 83 percent at 86.81 quorum for proposed CIP-011-3.[17] The NERC Board of Trustees adopted the proposed Reliability Standards on August 12, 2021.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standards would enhance reliability by providing increased options for entities to leverage third-party data storage and analysis systems in a secure manner, and are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The proposed revisions clarify the protections expected when using third-party solutions (e.g., cloud services). The following section discusses the revisions to the standards:

- proposed Reliability Standard CIP-004-7 (Subsection A);
- proposed Reliability Standard CIP-011-3 (Subsection B); and
- other modifications (Subsection C).

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

[16] The third drafts of the standards were posted as CIP-004-X and CIP-011-X because they were posted simultaneously with other proposed revisions to those standards as a part of Project 2016-02 Modifications to CIP Standards.

[17] The final drafts of the standards were posted as CIP-004-X and CIP-011-X because they were posted simultaneously with other proposed revisions to those standards as a part of Project 2016-02 Modifications to CIP Standards.

A. Proposed Reliability Standard CIP-004-7

As in currently effective Reliability Standard CIP-004-6, proposed Reliability Standard CIP-004-7 continues to include requirements that govern personnel risk assessment, training, security awareness, and access management in support of BES Cyber System security. The revisions in proposed CIP-004-7 include a new requirement on provisioned access to BCSI that consolidates access requirements previously spread throughout CIP-004-6. Proposed Reliability Standard CIP-004-7 includes six requirements: (1) Requirement R1 requires a Responsible Entity to implement a documented security awareness process for high and medium impact BES Cyber Systems that reinforces cyber security practices for certain personnel; (2) Requirement R2 requires Responsible Entities to implement a cyber security training program that includes the applicable requirement parts; (3) Requirement R3 requires a documented personnel risk assessment program(s); (4) Requirement R4 requires a documented access management program(s) that includes the applicable requirement parts; (5) Requirement R5 requires a documented access revocation program(s) that includes the applicable requirement parts; and (6) Requirement R6 is a new requirement that requires an access management program(s) to authorize, verify, and revoke provisioned access to BCSI that includes the applicable requirement parts.

The proposed revisions in CIP-004-7 center on removing references to "designated storage locations" and focusing the requirements on provisioned access to the BCSI, not just on where it is stored. This change permits entities to implement file-level rights and permissions, such as policy-based credentials or encryption, to manage access to BCSI. Provisioned access, while not proposed as a term in the NERC Glossary, is well understood among subject matter experts. Nevertheless, Requirement R6 clarifies that: "Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption

keys)." For example, an individual with encrypted BCSI but no encryption key has not been granted provisioned access to that BCSI because the Responsible Entity has not taken the step to give this individual the encryption key. Furthermore, while the individual has obtained the BCSI, the individual lacks the ability to use the BCSI without the key. Therefore, that individual does not have access to BCSI. Each Responsible Entity has its own process to grant provisioned access to individuals, and the concept of "provisioned access" in Requirement R6 is referring to the Responsible Entity's process.

Proposed CIP-004-7 includes revisions that eliminate the "designated storage locations" concept in order to facilitate more appropriate protections for using third-parties. To eliminate references to "designated storage locations," Requirement Part 4.4,[18] Part 5.3,[19] and subpart 4.1.3, from CIP-004-6 have been deleted in proposed CIP-004-7 and are incorporated into the new Requirement R6 on provisioned access, as described further below.[20] This centralizes all BCSI access requirements in the standard into one, new requirement. The proposed revised Part 4.1 with the deletion of subpart 4.1.3 reads as follows, in blackline:

> **4.1** Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
>
> **4.1.1** Electronic access; **and**
>
> **4.1.2** Unescorted physical access into a Physical Security Perimeter~~; and~~
>
> ~~**4.1.3** Access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

[18] The deleted Part 4.4 from CIP-004-6 reads as follows: Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

[19] The deleted Part 5.3 from CIP-004-6 reads as follows: For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

[20] Requirement 5.4 in CIP-004-6 becomes Requirement 5.3 in proposed CIP-004-7 as a result of this deletion.

Proposed new Requirement R6 applies to high impact BES Cyber Systems; medium impact BES Cyber Systems with External Routable Connectivity; and Electronic Access Control or Monitoring Systems ("EACMS") and Physical Access Control Systems ("PACS") associated with these high and medium BES Cyber Systems. Proposed new Requirement R6 reads as follows:

> **R6.** Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information.* To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

There are three new requirement parts within Requirement R6. Proposed Part 6.1 requires Responsible Entities to authorize provisioned electronic access and provisioned physical access to BCSI. Proposed Part 6.2 incorporates into the access management program the deleted Part 4.4 obligations to verify individuals with provisioned access are still appropriate. Finally, proposed Part 6.3 incorporates into the provisioned access program the deleted Part 5.3 obligation to remove an individual's ability to use provisioned access to BCSI for a termination action. Proposed Parts 6.1, 6.2, and 6.3 provide as follows:

> **6.1** Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
>
> **6.1.1.** Provisioned electronic access to electronic BCSI; and
>
> **6.1.2.** Provisioned physical access to physical BCSI.
>
> **6.2** Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:

6.2.1. have an authorization record; and

6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.

6.3 For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

B. Proposed Reliability Standard CIP-011-3

Proposed Reliability Standard CIP-011-3 addresses information protection of BCSI and includes two requirements. Proposed Requirement R1 requires Responsible Entities to implement a documented information protection program(s) that includes the applicable requirement parts. Proposed Requirement R2 requires Responsible Entities to implement documented processes regarding BES Cyber Asset reuse and disposal, consistent with the applicable requirement parts. Proposed Requirement R1 includes the only substantive modifications to CIP-011-3, which are shown in blackline below:

R1. Each Responsible Entity shall implement one or more documented information protection program(s) **for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program*** that collectively includes each of the applicable requirement parts in *CIP-011-~~2~~3 Table R1 – Information Protection **Program**. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

The language added to Requirement R1 helps scope the applicability of the requirement parts to the BCSI pertaining to the systems listed in the applicability column of Table R1 – Information Protection Program. This clarifies the intent of the requirement to place protections around the BCSI, regardless of its storage location. This revision permits Responsible Entities to leverage more appropriate protections for use with third parties.

Within Requirement R1, proposed CIP-011-3 Table R1 – Information Protection Program includes two modified requirement parts. Proposed Parts 1.1 and 1.2 apply to high and medium

impact BES Cyber Systems and their associated EACMS and PACS. Proposed Parts 1.1 and 1.2 provide as follows, in blackline:

> **1.1** Method(s) to identify **BCSI** ~~information that meets the definition of BES Cyber System Information~~.
>
> **1.2** ~~Procedure(s) for protecting and~~ **Method(s) to protect and** securely handl~~e~~**ing** **BCSI to mitigate the risks of compromising confidentiality** ~~BES Cyber System Information, including storage, transit, and use~~.

The proposed changes to Parts 1.1 and 1.2 clarify and simplify the requirement language. Proposed Part 1.1 removes redundant language. Proposed Part 1.2 includes more objective-level language to once again focus the protections on the BCSI itself. The proposed objective of Part 1.2 is "to mitigate the risks of compromising confidentiality." The intent of proposed Part 1.2 is to protect BCSI from unauthorized access no matter where the BCSI is located or its state (i.e., in storage, transit, or use). Therefore, in focusing protections on preserving confidentiality, the requirements in proposed CIP-011-3 help ensure that BCSI is protected regardless of the location of the BCSI.

C. 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.

First, the Interchange Coordinator or Interchange Authority is removed from the Applicability section of the proposed Reliability Standards. This revision is consistent with FERC-approved changes to the NERC Compliance Registry under the risk-based registration initiative.[21]

---

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

Second, the term "Special Protection Systems" has been replaced in the Applicability section of the proposed Reliability Standards with the term "Remedial Action Schemes," consistent with similar revisions made to other NERC Reliability Standards.[22]

Third, the acronym for BES Cyber System Information, BCSI, has replaced all references to BES Cyber System Information except in certain circumstances, such as first use of the term and in headers of some tables. Responsible Entities often use the acronym BCSI when implementing these requirements. As such, the standard drafting team determined to incorporate the acronym to better reflect usage in industry.

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

D. 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.

---

[22] *See Notice of Filing of the North American Electric Reliability Corporation of Revisions to the Definition of "Remedial Action Scheme" and Proposed Reliability Standards*, (Feb. 25, 2015) (NERC provided notice of revised definition of the term "Remedial Action Scheme" and certain Reliability Standards in which references to the term "Special Protections Systems" were removed and replaced with the term "Remedial Action Schemes").

V. EFFECTIVE DATE

The proposed Reliability Standards shall become effective as 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 standard shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction. The 24-month implementation period is designed to afford Responsible Entities sufficient time to implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services; establish or modify vendor relationships to ensure compliance with the new and revised requirements in proposed CIP-004-7 and CIP-011-3; and make the necessary administrative changes, such as revising their information protection programs to incorporate the new requirements.

The proposed Implementation Plan also permits Responsible Entities to elect to comply with proposed CIP-004-7 and CIP-011-3 following applicable governmental entity approval but prior to the standards' effective date, provided the Responsible Entity notifies its applicable Regional Entities. Some Responsible Entities desire to use third party services for BCSI sooner than the effective date, and early adoption of CIP-004-7 and CIP-011-3 would allow Responsible Entities to implement the appropriate controls commensurate with third-party use.

VI. CONCLUSION

For the reasons set forth above, NERC respectfully requests approval of:

- proposed Reliability Standards CIP-004-7, and CIP-011-3, and associated elements included in Exhibit A, effective as proposed herein;
- the proposed Implementation Plan included in Exhibit B; and
- the retirement of Reliability Standards CIP-004-6 and CIP-011-2, effective as proposed herein.

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: September 23, 2021

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 require Responsible Entities to manage access to BES Cyber Security Information ("BCSI") to prevent unauthorized use. To manage this access, the proposed Reliability Standards provide increased options for Responsible Entities to leverage third-party data storage and analysis systems to store BCSI in a secure manner. As a result, the proposed Reliability Standards enhance reliability by still requiring protections around access to BCSI while permitting Responsible Entities the flexibility to securely use third-party data storage and analysis systems.

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 G**. 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.

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 would achieve the reliability goal of protecting BCSI through managing access to it.

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 permit Responsible Entities to leverage more types of protections to secure BCSI, including encryption.

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 comply to develop necessary processes. The proposed implementation plan also permits Responsible Entities to early adopt the revisions once approved by the applicable governmental authority and upon notification of applicable Regional Entities.

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 H** 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 request for approval of the 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.