NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 22, 2020

VIA ELECTRONIC FILING

Rachelle Verret Morphy
Saskatchewan Electric Reliability Authority
2025 Victoria Avenue
Regina, Saskatchewan, Canada S4P 0S1

Re: *North American Electric Reliability Corporation*

Dear Ms. Morphy:

The North American Electric Reliability Corporation ("NERC") hereby submits Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standard CIP-002-6. 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.

Respectfully submitted,

/s/ Lauren Perotti

Lauren Perotti
Senior Counsel for the North American Electric Reliability Corporation

Enclosure

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BEFORE THE
CROWN INVESTMENT CORPORATION
OF THE PROVINCE OF SASKATCHEWAN

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

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARD CIP-002-6

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

June 22, 2020

TABLE OF CONTENTS

I. SUMMARY 2

II. NOTICES AND COMMUNICATIONS 3

III. BACKGROUND 4

A. NERC Reliability Standards Development Procedure 4

B. CIP Version 5 Transition Program Recommendations 4

C. Development of the Proposed Reliability Standard 6

IV. JUSTIFICATION 8

A. Modifications to Attachment 1, Criterion 2.12 8

B. Other Modifications 12

C. Enforceability of Proposed Reliability Standard 13

V. EFFECTIVE DATE 14

Exhibit A Proposed Reliability Standard

Exhibit B Implementation Plan

Exhibit C Reliability Standards Criteria

Exhibit D Analysis of Violation Risk Factors and Violation Severity Levels

Exhibit E Summary of Development History and Complete Record of Development

Exhibit F Transmission Owner Control Center White Paper

Exhibit G Standard Drafting Team Roster

BEFORE THE
CROWN INVESTMENT CORPORATION
OF THE PROVINCE OF SASKATCHEWAN

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION)
)

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARD CIP-002-6

The North American Electric Reliability Corporation ("NERC") hereby submits proposed Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization. Proposed Reliability Standard CIP-002-6 clarifies the criterion for determining which BES Cyber Systems associated with Transmission Owner Control Centers performing the functional obligations of a Transmission Operator fall under the medium impact category.[1] The proposed Reliability Standard, provided in Exhibit A hereto, is just, reasonable, not unduly discriminatory or preferential, and in the public interest.

NERC also provides notice of:

- the associated implementation plan (Exhibit B);
- the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A and D); and
- the retirement of Reliability Standard CIP-002-5.1a.

[1] 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.

This filing presents the technical basis and purpose of the proposed Reliability Standard, a summary of the development history (Exhibit E), and a demonstration that the proposed Reliability Standard meets the Reliability Standards criteria (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standard on May 14, 2020.

I. SUMMARY

NERC's cyber security Critical Infrastructure Protection ("CIP") Reliability Standards seek to mitigate cyber security risks to Bulk Electric System ("BES") Facilities, systems, and equipment. To address these risks, the cyber security CIP standards focus on protections around BES Cyber Systems. Responsible Entities[2] categorize BES Cyber Systems as low, medium, or high impact based on the characteristics of their BES Facilities, systems, and equipment. BES Cyber Systems used by and located at certain Control Centers are high impact, and BES Cyber Systems associated with certain other BES Facilities, systems, and equipment are medium or low impact. Depending on the assigned impact level, Responsible Entities then apply corresponding requirements from the CIP Reliability Standards to their BES Cyber Systems or the assets containing those BES Cyber Systems.

Proposed Reliability Standard CIP-002-6 includes the criteria for determining the impact level of BES Cyber Systems and is foundational for understanding the applicability of the suite of CIP Reliability Standards. Proposed CIP-002-6 has two requirements that remain substantively unchanged from CIP-002-5.1a. Proposed Requirement R1 requires Responsible Entities to implement a process to review certain assets, such as Control Centers and Transmission stations and substations, among others, and identify the impact level of the assets' BES Cyber Systems

[2] 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.

according to Attachment 1 to the Reliability Standard. Proposed Requirement R2 requires Responsible Entities to review these identifications performed pursuant to Requirement R1 at least once every 15 calendar months and obtain CIP Senior Manager, or delegate, approval of these identifications and reviews.

Proposed Reliability Standard CIP-002-6 improves upon CIP-002-5.1a by clarifying the criterion for Transmission Owner Control Centers and tailoring the language to better reflect the risk posed by these Control Centers if unavailable or compromised. Throughout implementation of CIP-002-5.1a, NERC staff and industry stakeholders observed that not all Control Centers meeting Criterion 2.12 posed the same level of risk. As a result, the revisions in proposed CIP-002-6 include changes to medium impact Criterion 2.12 in Attachment 1 and other minor modifications. Proposed Reliability Standard CIP-002-6 enhances BES reliability by providing for improved risk identification, which in turn permits Responsible Entities to focus their resources on protecting assets that pose a higher risk to reliability if unavailable or compromised.

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 of 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

The following background information is provided below: (1) a description of the NERC Reliability Standards Development Procedure; (2) an overview of the need for revisions to CIP-002; and (3) the history of the Project 2016-02 Modifications to CIP Standards.

A. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was 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.[3] 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 satisfy 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 Board is required before NERC submits the Reliability Standard to the applicable governmental authorities.

B. CIP Version 5 Transition Program Recommendations

In 2013, NERC initiated the CIP Version 5 Transition Program in collaboration with industry stakeholders and Regional Entities to assist Responsible Entities with implementation of the "Version 5" CIP Reliability Standards.[4] As part of this program, industry volunteers

[3] 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/FilingsOrders/us/RuleOfProcedureDL/SPM_Clean_Mar2019.pdf.

[4] The "Version 5" Reliability Standards refer to CIP-002-5.1, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1.

participated in an implementation study under which they would adopt the Version 5 standards prior to their effective date.[5] The implementation study afforded NERC and industry the opportunity to assess potential issues with implementation of the Version 5 standards to help ensure Responsible Entities could transition smoothly to the new requirements.

NERC worked with the industry implementation study participants, Regional Entity staff, and the United States Federal Energy Regulatory Commission ("FERC") staff to develop lessons learned from early implementation of the Version 5 standards. Throughout 2014 and 2015, this group, the Version 5 Transition Advisory Group ("V5 TAG"), developed documents with the lessons learned and frequently asked questions.[6] In addition, the V5 TAG identified implementation issues that would best be addressed through standards revisions.[7]

Among other things, the V5 TAG recommended clarifying certain language in Attachment 1 to CIP-002-5.1a. Specifically, the V5 TAG suggested revisions to the language italicized below within medium impact Criterion 2.12 of CIP-002-5.1a:

> Each Control Center or backup Control Center *used to perform the functional obligations of* the Transmission Operator not included in High Impact Rating (H), above. [emphasis added]

The V5 TAG observed that the phrase "used to perform the functional obligation of" was particularly unclear for Transmission Owners who may only operate limited breakers for assets containing low impact BES Cyber Systems. Based on the language of the Criterion 2.12 in CIP-002-5.1a, these Transmission Owners' Control Centers could be considered to contain medium

---

[5] NERC, *Implementation Study Final Report – CIP Version 5 Transition Program* (Oct. 2014), https://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf.

[6] The V5 TAG lessons learned and frequently asked questions documents are available at https://www.nerc.com/pa/CI/Pages/Transition-Program-V5-Implementation-Study.aspx.

[7] NERC, *CIP V5 Issues for Standard Drafting Team Consideration* (Sept. 15, 2015), https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/Transfer_Issues_V5TAG-SDT_1st-final-03232016.pdf.

impact BES Cyber Systems despite operating a few assets with low impact BES Cyber Systems. As discussed further in the Transmission Owner Control Center White Paper (Exhibit F), the V5 TAG determined that this language in CIP-002-5.1a should be clarified.

C. Development of the Proposed Reliability Standard

As further described in Exhibit E hereto, NERC initiated a standard development project, Project 2016-02 Modifications to CIP Standards ("Project 2016-02"), and appointed a standard drafting team (Exhibit G) to address the directives from FERC Order No. 822[8] as well as issues identified during implementation of the CIP Reliability Standards approved in FERC Order No. 791.[9] NERC developed a Standard Authorization Request ("SAR") that detailed the scope of Project 2016-02. One issue identified in the SAR included clarification of the applicability of requirements to a Control Center of a Transmission Owner that performs the functional obligations of a Transmission Operator, as described in subsection C above. The standard drafting team addressed this issue in revisions to Criterion 2.12 of Attachment 1 to CIP-002-5.1a.

On September 14, 2017, NERC posted the initial draft of proposed Reliability Standard CIP-002-6 for a 45-day comment period, which included an initial ballot during the last 10 days of the comment period. The initial ballot of CIP-002-6 received the requisite approval with affirmative votes of 66.78 percent of the ballot pool. After considering comments on the initial draft, NERC posted a second draft of CIP-002-6 for an additional 45-day comment period and ballot on March 16, 2018, which included an additional ballot during the last 10 days of the

---

[8] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, *order denying reh'g,* 156 FERC ¶ 61,052 (2016).

[9] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

comment period. The second draft of proposed Reliability Standard CIP-002-6 received the requisite approval with affirmative votes of 93.31 percent of the ballot pool.

Because another standards development project, Project 2015-09 Establish and Communicate System Operating Limits, required revisions to the impact rating criteria, the Project 2016-02 standard drafting team incorporated the additional revisions to avoid simultaneous postings of different revisions within CIP-002-6. The standard drafting team posted CIP-002-6 on August 23, 2018 for another 45-day comment period, which included an initial ballot during the last 10 days of the comment period. This initial ballot of CIP-002-6 did not receive the requisite approval of the ballot pool. After considering the comments received, the teams from both projects determined not to include in CIP-002-6 the language suggested by the Project 2015-09 standard drafting team.

A fourth draft of proposed Reliability Standard CIP-002-6 was then posted for a 45-day additional comment period and ballot on June 3, 2019, which included an additional ballot during the last 10 days of the comment period. The fourth draft of proposed Reliability Standard CIP-002-6 received the requisite approval with affirmative votes of 87.39 percent of the ballot pool. After considering comments received, the standard drafting team determined to further revise the Reliability Standard and post for an additional comment period and ballot.

A fifth draft of proposed Reliability Standard CIP-002-6 was posted for a 45-day additional comment period and ballot on November 1, 2019, which included an additional ballot during the last 10 days of the comment period. The fifth draft of proposed Reliability Standard CIP-002-6 received the requisite approval with affirmative votes from 95.98 percent of the ballot pool. After considering comments received, the standard drafting team determined to proceed to final ballot.

On March 26, 2020, NERC conducted a ten-day final ballot for proposed Reliability Standard CIP-002-6, which received affirmative votes from 96.28 percent of the ballot pool. The Board adopted the proposed Reliability Standard on May 14, 2020.

IV. JUSTIFICATION

As discussed below and in Exhibit C, proposed Reliability Standard CIP-002-6 clarifies the impact level criterion for certain Control Centers and is just, reasonable, not unduly discriminatory or preferential, and in the public interest. This section discusses the following: the modifications to Attachment 1, Criterion 2.12 (Section IV.A) and other clarifying modifications (Section IV.B). This section concludes with a discussion of the enforceability of the proposed Reliability Standard (Section IV.C).

A. Modifications to Attachment 1, Criterion 2.12

Proposed Requirement R1 in CIP-002-6 requires Responsible Entities to implement a process to identify the impact rating of BES Cyber Systems. Proposed Requirement R1 and Parts 1.1 through 1.3 require Responsible Entities to identify the BES Cyber Systems according to Attachment 1. As noted above, proposed Requirement R1 remains substantively unchanged from CIP-002-5.1a. The substantive revisions in proposed CIP-002-6 are reflected in the referenced attachment, Attachment 1. Consistent with the recommendations from the V5 TAG, proposed CIP-002-6 includes revisions to Criterion 2.12 of Attachment 1 to clarify which BES Cyber Systems associated with Control Centers owned by Transmission Owners that perform the functional obligations of a Transmission Operator should be categorized as medium impact.

Proposed Requirement R1 reads as follows:

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. Remedial Action Schemes that support the reliable operation of the Bulk Electric System; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1 Identify each of the high impact BES Cyber System according to Attachment 1, Section 1, if any, at each asset;

1.2 Identify each of the medium impact BES Cyber System according to Attachment 1, Section 2, if any, at each asset; and

1.3 Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Attachment 1 includes criteria characterizing the level of impact of the BES Cyber Systems used by and located at certain assets for high impact BES Cyber Systems and associated with certain assets for low and medium impact BES Cyber Systems. In the medium impact section of the attachment, Criterion 2.12 addresses how BES Cyber Systems associated with Control Centers that perform the functional obligations of the Transmission Operator ("TOP") must be categorized. Proposed Criterion 2.12 focuses on the span of control of the BES Cyber Systems rather than the tasks of the TOP functional registration. In so doing, the criterion more appropriately bases the impact rating on the risk of the BES Cyber Systems associated with the Control Center. Proposed Criterion 2.12 reads as follows, with proposed revisions in blackline:

2.12. Each Control Center or backup Control Center**, not included in the High Impact Rating,** used to perform the ~~functional obligations~~ **reliability tasks** of ~~the~~ **a** Transmission Operator **in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center** ~~not included in High Impact Rating (H), above~~.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

To help assess the risk posed by the BES Cyber Systems associated with a Control Center, the standard drafting team assigned a weight value to the Transmission Lines that a Control Center monitors and controls, as portrayed in the table included in Criterion 2.12. The standard drafting team mimicked the approach used in Criterion 2.5 to assign weighted values to Transmission Lines. For Criterion 2.5, the total aggregate weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines or five connected 230 kV lines at a single Transmission station or substation.[10] The associated BES Cyber Systems of a single Transmission station or substation with lines having an aggregate weighted value greater than 3,000 would be categorized as medium impact according to Criterion 2.5.

The standard drafting team used the logic behind Criterion 2.5 and applied it in the context of Control Centers for proposed Criterion 2.12. By definition, a "Control Center" performing the reliability tasks of a TOP monitors and controls Transmission Facilities at two or more locations. Based on the "two or more locations" threshold, the standard drafting team concluded that doubling the aggregate weighted value of lines at a single Transmission station or substation that

[10] The weight in Criterion 2.5 was based on a document regarding determining Severity Risk Index developed by a working group of the NERC Planning Committee: *NERC Planning Committee Reliability Metrics Working Group*, Integrated Risk Assessment Approach – Refinement to Severity Risk Index (May 2011), available at https://www.nerc.com/docs/pc/rmwg/SRI_Equation_Refinement_May6_2011.pdf.

meets the medium impact criteria would provide an appropriate floor for this criterion that is commensurate with the risk posed by these Control Centers. Doubling the weighted value means the threshold is greater than 6,000 for Control Centers that monitor at least two or more of these Facilities. Furthermore, proposed Criterion 2.12 accounts for BES Cyber Systems associated with Control Centers that have not already been classified as high impact. As a result, any Transmission Facility controlled by a Control Center meeting Criterion 2.12 would have BES Cyber Systems that fall into the low impact category.

To confirm that the proposed criterion was commensurate with the risk of the Control Centers, NERC performed an analysis of Transmission Owners and Transmission Operators affected by an aggregate weighted value of less than and near 6,000 by using NERC's data. Seven entities total were selected from the Eastern, Western, and Texas Interconnections. The analysis simulated a compromised Control Center by simultaneously opening all Transmission lines owned by their respective Transmission Owner or Transmission Operator and monitored electrically adjacent BES elements for adverse reliability impacts associated with thermal overloads. This was a Steady-State analysis that locked generator, transformer taps, and switchable shunt devices to ensure more immediate potential impacts to the Bulk-Power System could be monitored. In all cases studied, nearby areas showed voltage and frequency in oversupply due to the net loss of load compared to generation in the affected area. Oversupply system conditions are more easily remedied by backing down neighboring generation as opposed to ramping up generation or shedding load from undersupply system conditions. Based on the dataset used, the analysis found the following:

- No low voltage issues;

- High voltage issues could be remedied in Operations through backing down of generation whereby ramp down times are minimal in all situations; and
- Screen indicated no issues with thermal overloads of nearby buses and would not trigger adjacent protection systems.

Based on these results, NERC determined that the proposed criterion was commensurate with the risk posed by the assets.

B. Other Modifications

Proposed Reliability Standard CIP-002-6 also contains a number of minor modifications to align the standard 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 proposed Reliability Standard CIP-002-6. This revision is consistent with changes to the NERC Compliance Registry under the risk-based registration initiative.[11]

Second, the term "Special Protection Systems" has been replaced with the term "Remedial Action Schemes," consistent with similar revisions made to other NERC Reliability Standards.[12] This change occurs in the following locations:

- Applicability subsections 4.1.2.2 and 4.2.1.2;
- Requirement R1;

---

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

[12] *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), in which NERC provided notice of NERC's revised definition of the term "Remedial Action Scheme" and that references to the term "Special Protections Systems" were removed and replaced with the term "Remedial Action Schemes" in certain Reliability Standards.

- medium impact rating criterion 2.9; and
- low impact rating criterion 3.5.

Third, proposed Requirement R2 begins with the word "**Each** Responsible Entity shall:", instead of "~~**The**~~ Responsible Entity shall:", to conform with Requirement R1 language and other requirements in the CIP suite of standards.

Fourth, proposed CIP-002-6 carries forward the interpretation of CIP-002-5.1a regarding Criterion 2.1.[13] In Appendix 1 to CIP-002-5.1a, and now proposed CIP-002-6, the interpretation provides clarity regarding the phrase "shared BES Cyber Systems" as used in Criterion 2.1. The standard drafting team determined that it was appropriate to apply the interpretation from CIP-002-5.1a to proposed CIP-002-6 rather than incorporate additional edits into the proposed requirements.

Finally, proposed CIP-002-6 includes other minor modifications to the non-enforceable sections of the standard.

C. Enforceability of Proposed Reliability Standard

The proposed Reliability Standard also includes measures that support the requirements by clearly identifying what is required and how the ERO will enforce the requirements. The 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 Standard includes VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard did not change from the VRFs and VSLs in CIP-002-5.1a and

[13] *See Notice of Filing of the North American Electric Relability Corporation of Interpretation of Reliability Standard CIP-002-5.1a (Nov. 29, 2016).*

continue to comport with NERC and FERC guidelines related to their assignment, as shown in Exhibit D.

V. EFFECTIVE DATE

The proposed Reliability Standard becomes effective as set forth in the proposed Implementation Plan, provided in Exhibit B hereto. Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter immediately 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 immediately after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

If the revisions to Criterion 2.12 of Attachment 1 to CIP- 002- 6 result in a higher impact level categorization of a BES Cyber System, a Responsible Entity shall identify that BES Cyber System as a higher categorization and apply the requirements within 24 months after the effective date of CIP-002-6. Until the Responsible Entity has implemented the protections required under the higher categorization, the Responsible Entity shall continue to identify that BES Cyber System consistent with its existing categorization under CIP- 002- 5.1a, Requirement R1, Part 1.3.

If the impact level categorization is the same or lower, Responsible Entities are expected to continue to apply the same protections as CIP-002-5.1a or apply lower categorization protections as soon as proposed CIP-002-6 becomes effective, if applicable. In addition, the proposed Implementation Plan includes a provision where Responsible Entities shall initially comply with the periodic requirements in CIP- 002- 6, Requirement R2 within 15 calendar

months of their last performance of Requirement R2 under CIP- 002- 5.1a. This provision has the effect of allowing Responsible Entities to maintain their existing review schedule of every 15 calendar months or fewer.

Finally, the proposed Implementation Plan carries forward the provisions governing planned and unplanned changes from the Implementation Plan associated with CIP-002-5.1a, with certain conforming changes. The implementation period is designed to afford Responsible Entities time to incorporate the updated requirements into their processes while balancing the need for expeditious implementation of proposed CIP-002-6.

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: June 22, 2020

EXHIBITS A - B and D - G

EXHIBIT C

Reliablity Standards Criteria

The discussion below explains how the proposed Reliability Standard meets or exceeds 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 Standard identifies and categorizes Bulk Electric System ("BES") Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems supports appropriate protection against compromises that could lead to misoperation or instability in the BES. Specifically, the proposed Reliability Standard clarifies the criterion for determining which BES Cyber Systems associated with Transmission Owner Control Centers performing the functional obligations of a Transmission Operator fall under the medium impact category. The Project 2016-02 standard drafting team, comprised of industry experts, incorporated an approach used in another criterion based on studies, and NERC validated the approach through its own study, to provide a technically sound basis for the proposed revisions.

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 Standard is clear and unambiguous as to what is required and who is required to comply. The proposed Reliability Standard applies to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators,

Transmission Operators, and Transmission Owners. The proposed Reliability Standard clearly articulates 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 and Violation Severity Levels ("VSLs") for the proposed Reliability Standard 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 Standard includes 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 Standard contains 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 Standard achieves the reliability goals effectively and efficiently. The proposed Reliability Standard clearly articulates the security objective that applicable entities

must meet while permitting entities to apply a risk-based approach to the categorization of BES Cyber Systems.

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 Standard does not reflect a "lowest common denominator" approach. The proposed Reliability Standard helps to ensure that entities allocate resources commensurate with the adverse impact that loss, compromise, or misuse of BES Cyber Systems could have on the reliable operation of the BES.

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 Standard applies throughout North America and does 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 Standard has no undue negative impact on competition. The proposed Reliability Standard requires the same performance by each of the applicable Functional Entities. The proposed Reliability Standard does 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 Standard 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 BES Cyber Systems that are a higher categorization as a result of the proposed revisions.

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

The proposed Reliability Standard was 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 Standard. 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 Standard. No comments were received that indicated the proposed Reliability Standard conflicts 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 Standard is just and reasonable were identified.