NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 29, 2019

VIA ELECTRONIC FILING

Michael Law
President and Chief Executive Officer
Alberta Electric System Operator
2500, 330 - 5 Avenue SW
Calgary, Alberta
T2P 0L4

RE: *North American Electric Reliability Corporation*

Dear Mr. Law:

The North American Electric Reliability Corporation ("NERC") hereby submits Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standard CIP-003-8. NERC requests, to the extent necessary, a waiver of any applicable filing requirements with respect to this filing.

NERC understands the AESO may adopt the proposed reliability standards subject to Alberta legislation, principally as established in the *Transmission Regulation* ("the T Reg."). Briefly, it is NERC's understanding that the T Reg. requires the following with regard to the adoption in Alberta of a NERC Reliability Standard:

1. The AESO must consult with those market participants that it considers are likely to be directly affected.

2. The AESO must forward the proposed reliability standards to the Alberta Utilities Commission for review, along with the AESO's recommendation that the Commission approve or reject them.

3. The Commission must follow the recommendation of the AESO that the Commission approve or reject the proposed reliability standards unless an interested person satisfies the Commission that the AESO's recommendation is "technically deficient" or "not in the public interest."

Further, NERC has been advised by the AESO that the AESO practice with respect to the adoption of a NERC Reliability Standard includes a review of the NERC Reliability Standard for applicability to Alberta legislation and electric industry practice. NERC has been advised that, while the objective is to adhere as closely as possible to the requirements of the NERC Reliability Standard, each NERC Reliability Standard

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

approved in Alberta (called an "Alberta reliability standard") generally varies from the similar and related NERC Reliability Standard.

NERC requests the AESO consider Proposed Reliability Standard CIP-003-8 in the filing for adoption in Alberta as an "Alberta reliability standard(s)," subject to the required procedures and legislation of Alberta.

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

BEFORE THE
ALBERTA ELECTRIC SYSTEM OPERATOR

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

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARD CIP-003-8

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

May 28, 2019

TABLE OF CONTENTS

BEFORE THE
ALBERTA ELECTRIC SYSTEM OPERATOR

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

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARD CIP-003-8

The North American Electric Reliability Corporation ("NERC") hereby submits proposed Reliability Standard CIP-003-8 – Cyber Security – Security Management Controls. The proposed Reliability Standard addresses the Federal Energy Regulatory Commission's ("FERC") directive from Order No. 843 to develop modifications to CIP-003-8 to mitigate the risk of malicious code that could result from third-party transient electronic devices for low impact BES Cyber Systems.[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-003-7.

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

[1] 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.

Standard meets the Reliability Standards criteria (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standard on May 9, 2019.

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 located at or associated with BES Facilities, systems, and equipment. Responsible Entities[2] categorize BES Cyber Systems as low, medium, or high impact based on the characteristics of their BES Facilities, systems, and equipment. 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.

Reliability Standard CIP-003-7 requires entities to adopt and maintain cyber security policies for the areas covered under the other CIP cyber security standards. The purpose of these policies is to communicate management goals, objectives, and expectations for protecting BES Cyber Systems. Reliability Standard CIP-003-7 also contains all of the requirements applicable to low impact BES Cyber Systems. Requirement R2 of CIP-003-7 requires Responsible Entities to implement cyber security plans for low impact BES Cyber Systems that address the following areas: (1) cyber security awareness; (2) physical security; (3) electronic access; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media malicious code risk mitigation.

---

[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.

Proposed Reliability Standard CIP-003-8 improves upon CIP-003-7 by explicitly requiring Responsible Entities to implement those actions they deem necessary to mitigate the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets managed by third parties, such as vendors or contractors. The Responsible Entity must determine which actions, if any, are necessary based on a review of the third party's mitigation practices. Additionally, the Responsible Entity must implement the action before connecting the Transient Cyber Asset to its low impact BES Cyber System. The proposed requirement helps ensure that Responsible Entities protect their low impact BES Cyber Systems at an appropriate level of security when allowing other parties to use their own Transient Cyber Assets at low impact BES Cyber Systems.

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 FERC's directive from Order No. 843 addressed in this filing; 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 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 for approval.

B. Order No. 843 Directive

In Order No. 843, FERC approved Reliability Standard CIP-003-7.[4] NERC developed Reliability Standard CIP-003-7 to address directives from Order No. 822 regarding electronic access controls and protection of transient devices for low impact BES Cyber Systems. In approving CIP-003-7, FERC found that NERC improved upon CIP-003-6 by: (1) clarifying electronic access controls for low impact BES Cyber Systems; (2) developing controls for Transient Cyber Assets and Removable Media used at low impact BES Cyber Systems; and (3) requiring a policy for CIP Exceptional Circumstances related to low impact BES Cyber Systems.[5]

---

[3] 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 https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/SPM_Clean_Mar2019.pdf.

[4] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Order No. 843, 163 FERC ¶ 61,032, P 17 (2018) ("Order No. 843")..

[5] *Revised Critical Infrastructure Protection reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, at P 17, *order on reh'g,* 156 FERC ¶ 61,052 (2016).

FERC, however, expressed concern that CIP-003-7 lacked a clear requirement to mitigate the risk of malicious code that could result from third-party transient electronic devices. FERC noted that CIP-003-7 did not explicitly require Responsible Entities to: (1) mitigate any malicious code found during review of the third-party mitigation measures; or (2) take reasonable steps to mitigate risks of third-party malicious code, if the third party was not able to do so.[6] As a result, FERC directed NERC to develop and submit modifications to the NERC Reliability Standards to explicitly require Responsible Entities to implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices.[7]

C. Development of the Proposed Reliability Standard

As further described in Exhibit E hereto, NERC developed a Standard Authorization Request to address FERC's Order No. 843 directive and assigned it to the existing Project 2016-02 standard drafting team.[8] On August 23, 2018, NERC posted the initial draft of proposed Reliability Standard CIP-003-8 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-003-8 received the requisite approval, with 90.06 percent affirmative votes and 79.01 percent quorum. On April 18, 2019, NERC conducted a ten-day final ballot for proposed Reliability Standard CIP-003-8, which received affirmative votes of 91.44 percent of the ballot pool and 83.64 percent quorum. The Board adopted the proposed Reliability Standard on May 9, 2019.

---

6 Order No. 843 at P 32.

7 *Id.* at P 39.

8 The roster for the Project 2016-02 standard drafting team is included as Exhibit F to this filing.

IV. JUSTIFICATION

As discussed below and in Exhibit C, proposed Reliability Standard CIP-003-8 addresses FERC's directive in Order No. 843 to explicitly require Responsible Entities to implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices. Proposed CIP-003-8 helps to improve the cyber security posture of Responsible Entities using third-party services and is just, reasonable, not unduly discriminatory or preferential, and in the public interest. This section discusses the following:

- modifications to the Requirements of CIP-003 to address the Order No. 843 directive (Subsection A);
- modifications to the applicability of CIP-003 (Subsection B); and
- the enforceability of the proposed Reliability Standard (Subsection C).

A. Modifications Addressing the Directive

Consistent with Order No. 843, proposed CIP-003-8 includes additional requirements applicable to Responsible Entities with low impact BES Cyber Systems to mitigate the risks of the introduction of malicious code from third-party Transient Cyber Assets. To address the directive from Order No. 843, proposed Section 5 includes a new subsection 5.2.2 and contains the following revisions, shown in bold and strikethrough text:

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;

- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any **~~,the use of~~:**

5.2.1 **Use** one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 **For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.**

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Under Section 5, prior to allowing third-party vendors or contractors to connect their Transient Cyber Assets to low impact BES Cyber Systems, subsection 5.2.1 requires Responsible Entities to use one or more methods to review the third party's mitigation of the introduction of malicious code. Based on this review, proposed subsection 5.2.2 requires Responsible Entities to

determine whether any additional mitigation actions are necessary to meet the Section 5 security objective and implement such actions prior to connecting the Transient Cyber Asset.

As noted in the filing of Reliability Standard CIP-003-7, Section 5 parallels language from Reliability Standard CIP-010-2, Attachment 1 regarding the mitigation of risk of malicious code from Transient Cyber Assets and Removable Media used at high and medium impact BES Cyber Systems.[9] The additional language in proposed subsection 5.2.2 also draws upon language from Reliability Standard CIP-010-2, Attachment 1. It is nearly identical to language from Section 2.3 of Attachment 1 to CIP-010-2, which states, "For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset."[10]

Consistent with FERC's directive from Order No. 843, proposed subsection 5.2.2 provides an additional level of security for low impact BES Cyber Systems and dispels any confusion over what actions a Responsible Entity must take. As NERC noted in its filing of CIP-010-2, Responsible Entities have less control over the management of third-party Transient Cyber Assets.[11] As such, requiring Responsible Entities to not only review the mitigation methods used by third parties but also to take any additional mitigation actions deemed necessary supports Responsible Entities in ensuring that third-party cyber security practices are on par with their own.

---

[9] *Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standard CIP-003-7* at 25-28, (Mar. 10, 2017).

[10] *Reliability Standard CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments* at 28, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-010-2&title=Cyber%20Security%20-%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments&jurisdiction=United%20States.

[11] *Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2* at 41-42, (Feb. 25, 2015).

As a result, proposed subsection 5.2.2 promotes a higher level of cyber security for low impact BES Cyber Systems while meeting FERC's directive from Order No. 843.

B. Alignment of Applicability

Proposed Reliability Standard CIP-003-8 also contains a number of minor modifications to the Applicability section to align the standard with revisions to other standards or initiatives in other areas.

First, the Interchange Coordinator or Interchange Authority is removed from the Applicability section of proposed Reliability Standard CIP-003-8. This revision is consistent with changes to the NERC Compliance Registry under the risk-based registration initiative.[12]

Second, the term "Special Protection Systems" in Applicability subsections 4.1.2.2 and 4.2.1.2 has been replaced with the term "Remedial Action Schemes," consistent with similar revisions made to other NERC Reliability Standards.[13]

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 requirement 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

---

[12] *N. Am. Elec. Reliability Corp.*, 150 FERC ¶ 61,213 (2015) (FERC approving removal of the Purchasing Selling Entity and Interchange Authority/Coordinator from the NERC Compliance Registry).

[13] *Notice of Filing of the North American Electric Reliability Corporation of Revisions to the Definiation of "Remedial Action Scheme" and Proposed Reliability Standards, (Feb. 25, 2015).* In Order No. 818, FERC approved NERC's revised definition of the term "Remedial Action Scheme" and approved certain Reliability Standards in which references to the term "Special Protections Systems" were removed and replaced with the term "Remedial Action Schemes". *Revisions to Emergency Operations Reliability Standards; Revisions to Undervoltage Load Shedding Reliability Standards; Revisions to the Definition of "Remedial Action Scheme" and Related Reliability Standards*, Order No. 818, 153 FERC ¶ 61, 228 (2015).

enforce the requirements of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard comport with NERC and FERC guidelines related to their assignment. Exhibit D provides the NERC and FERC guidelines and notes that the VRFs and VSLs in proposed CIP-003-8 did not change from the VRFs and VSLs in CIP-003-7.

V. EFFECTIVE DATE

The proposed Reliability Standard is to 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 proposed Reliability Standard shall become effective on the on the later of (1) January 1, 2020, or (2) the first day of the first calendar quarter that is six (6) calendar 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, Reliability Standard CIP-003-8 shall become effective on the later of (1) January 1, 2020, or (2) the first day of the first calendar quarter that is six (6) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction. 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-003-8.

Similar to other implementation plans for CIP standards, the proposed Implementation Plan associated with the proposed Reliability Standard addresses planned and unplanned changes and their impact on compliance with the requirements of CIP-003-8.[14] For CIP-003-8, the proposed

[14] For the purposes of the proposed associated Implementation Plan, planned and unplanned changes are defined in the Implementation Plan for Version 5 CIP Cyber Security Standards available at

Implementation Plan incorporates by reference the section regarding planned and unplanned changes from the Implementation Plan associated with CIP-003-7.[15]

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: May 28, 2019

https://www.nerc.com/pa/Stand/Project%20200806%20Cyber%20Security%20Order%20706%20DL/Implementation_Plan_clean_4_(2012-1024-1352).pdf. The proposed Implementation Plan for CIP-003-8 notes that future versions of Reliability Standard CIP-002-5.1a may address planned and unplanned changes that impact the suite of CIP Reliability Standards. As a result, the provision in the proposed Reliability Standard CIP-003-8 Implementation Plan may be superseded by the planned and unplanned changes section in future versions of Reliability Standard CIP-002-5.1a.

[15] *See Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standard CIP-003-7*, Exhibit C, (Mar. 10, 2017).

EXHIBITS A — B and D — F

EXHIBIT C

Reliability 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 improves upon the existing CIP Reliability Standards requiring mitigation of the risk of introduction of malicious code to BES Cyber Systems in satisfaction of the directive in Order No. 843.[1] Specifically, proposed Reliability Standard CIP-003-8 improves reliability by requiring Responsible Entities to take any additional actions deemed necessary to mitigate the risk of introduction of malicious code to low impact BES Cyber Systems through Transient Cyber Assets managed by a party other than the Responsible Entity. The proposed modifications parallel language in CIP-010-2, Attachment 1.

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.

---

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

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.

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 and provides entities the flexibility to tailor their plan(s) 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 Standard does not reflect a "lowest common denominator" approach. The proposed Reliability Standard satisfies FERC's directive in Order No. 843.

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 comply to develop and implement the necessary plans. Moreover, the implementation period is designed so that proposed CIP-003-8 does not take effect sooner than CIP-003-7 in relevant jurisdictions.

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 final ballot achieved a quorum and 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.