NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 10, 2016

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 hereby submits Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standard CIP-003-7. 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/ Shamai Elstein

Shamai Elstein
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-003-7

Shamai Elstein
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net
marisa.hecht@nerc.net
Counsel for the North American Electric Reliability Corporation

March 10, 2017

TABLE OF CONTENTS

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-003-7

The North American Electric Reliability Corporation ("NERC") hereby submits proposed Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls. The modifications in the proposed Reliability Standard address Federal Energy Regulatory Commission ("FERC") directives from Order No. 822 regarding: (1) electronic access control requirements for low impact BES Cyber Systems; and (2) protection for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected and disconnected from systems) used for low impact BES Cyber Systems.[1] Proposed Reliability Standard CIP-003-7, provided in Exhibit A hereto, is just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

NERC also provides notice of:

- revised definitions to be incorporated into the NERC Glossary for the following terms: (1) Removable Media; and (2) Transient Cyber Asset (Exhibit B);
- the associated Implementation Plan (Exhibit C);
- the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibit F); and

[1] Order No. 822 at PP 32, 73. Unless otherwise designated, all capitalized terms used herein shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

- the retirement of Reliability Standard CIP-003-6 and the NERC Glossary definitions of Low Impact External Routable Connectivity ("LERC") and Low Impact BES Cyber System Electronic Access Point ("LEAP").

This filing presents the technical basis and purpose of the proposed Reliability Standard, a summary of the development history (Exhibit G), and a demonstration that the proposed Reliability Standard meets the Reliability Standards criteria (Exhibit D). The NERC Board of Trustees ("Board") adopted proposed Reliability Standard CIP-003-7 on February 9, 2017.

I. EXECUTIVE SUMMARY

The purpose of NERC's cybersecurity Critical Infrastructure Protection ("CIP") Reliability Standards is to mitigate cybersecurity risks to Bulk Electric System ("BES") Facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cyber-attack would affect the reliable operation of the BES. The CIP Reliability Standards apply a risk-based construct, requiring Responsible Entities[2] to identify and categorize BES Cyber Systems as high, medium, or low impact, and then protect those BES Cyber Systems commensurate with the risks they present to the reliable operation of the BES.[3] Reliability Standard CIP-003-6, which was submitted on February 25, 2015, contains all the requirements applicable to low impact BES Cyber Systems, covering the following four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response.

The modifications in proposed Reliability Standard CIP-003-7 improve upon the existing protections applicable to low impact BES Cyber Systems, consistent with FERC's directives in

[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.

[3] See FERC Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*, 145 FERC ¶ 61,160, 78 Fed. Reg. 72,755 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

Order No. 822,[4] by: (1) clarifying the electronic access control requirements applicable to low impact BES Cyber Systems; (2) adding requirements related to the protection of transient electronic devices used for low impact BES Cyber Systems; and (3) requiring Responsible Entities to have a documented cyber security policy related to declaring and responding to CIP Exceptional Circumstances for low impact BES Cyber Systems. The following is a brief overview of the modifications in the proposed Reliability Standard:

Electronic Access Controls for Low Impact BES Cyber Systems – To reduce risks associated with uncontrolled communications to low impact BES Cyber Systems, Reliability Standard CIP-003-6 requires Responsible Entities to implement electronic access controls to permit only necessary inbound and outbound access to low impact BES Cyber Systems for certain communications using routable protocol.[5] Specifically, Section 3.1 of Attachment 1 to CIP-003-6 provides that where there is Low Impact External Routable Connectivity (or LERC), Responsible Entities must "implement a [Low Impact BES Cyber System Electronic Access Point (or a LEAP)] to permit only necessary inbound and outbound bi-directional routable protocol access."

The *NERC Glossary* term LERC defines the circumstances under which Responsible Entities must implement electronic access controls, or a LEAP, for low impact BES Cyber Systems.[6] As explained in the Guidelines and Technical Basis section appended to CIP-003-6 and NERC's pleadings in FERC Docket No. RM15-14-000, the LERC definition uses the term "direct" in the phrases "direct user-initiated interactive access" and "direct device-to-device connection" to distinguish between the scenarios where an external user or device could electronically access

[4] Order No. 822 at PP 32, 73.

[5] *See* CIP-003-6, Requirement R2, Attachment 1, Section 3. Under Section 3 of Attachment 1, Responsible Entities must also authenticate all Dial-up Connectivity that provides access to low impact BES Cyber System(s).

[6] The *NERC Glossary* definition of LEAP is "a Cyber Asset interface that controls [LERC]."

the low impact BES Cyber System without a security break (i.e., "direct" access) from those situations where an external user or device could only access the low impact BES Cyber System following a security break (i.e., "indirect" access).[7] As further explained, under CIP-003-6, Responsible Entities are required to implement a LEAP only when there is "direct" electronic access as there are no existing defenses to control access. In contrast, if an external user or device could only access the low impact BES Cyber System indirectly, there is no requirement to implement a LEAP.[8]

Although FERC approved CIP-003-6 and the LERC definition in Order No. 822, FERC also directed NERC to modify the LERC definition to reflect the clarification provided in the Guidelines and Technical Basis section and NERC's pleadings.[9] FERC expressed concern that absent such clarification, the use of the term "direct" in the LERC definition is ambiguous and could lead to complications in the implementation of the proposed CIP Reliability Standards, hindering the adoption of effective security controls for low impact BES Cyber Systems.[10]

In response to FERC's directive, NERC proposes to: (1) retire the *NERC Glossary* terms LERC and LEAP; and (2) modify Section 3 of Attachment 1 to CIP-003-7 to more clearly delineate the circumstances under which Responsible Entities must establish electronic access controls for low impact BES Cyber Systems. The proposed retirement of LERC and LEAP and modifications to Section 3 of Attachment 1 are designed to simplify the electronic access control requirements for low impact BES Cyber Systems to avoid the ambiguities associated with the term "direct" and help ensure that Responsible Entities implement the required security controls effectively.

---

7 *Comments of the North American Electric Reliability Corporation in Response to Notice of Proposed Rulemaking*, Docket No. RM15-14-000 at 28-31 (filed Sept. 21, 2015) ("NOPR Comments").

8 *Id*.

9 Order No. 822 ay PP 73-75.

10 Order No. 822 at PP 67, 73.

As explained in greater detail in Section IV.A below, the language in proposed Reliability Standard CIP-003-7 incorporates the concepts from the definitions of LERC and LEAP but does not distinguish between direct and indirect electronic access. Specifically, proposed Section 3 of Attachment 1 to CIP-003-7 simply provides that the Responsible Entity must implement electronic access controls for any communications, whether direct or indirect, "between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System" that use "a routable protocol when entering or leaving the asset containing the low impact BES Cyber System," unless that communication is "used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE)."

This simplified approach improves the clarity of the electronic access requirements by disentangling the type of communications requiring controls from controls that are already in place to address that communication. The existence of a complete security break is no longer used to determine whether electronic access controls are required; instead, the use of a complete security break is treated as another form of electronic access control that is intended to meet the security objective. The proposed modifications avoid overemphasis on identifying LERC and focuses Responsible Entities on the security objective of the requirement. Importantly, the proposed modifications to Section 3 of Attachment 1 and the retirement of LERC and LEAP do not alter the security objective of or the controls required by Section 3 of Attachment 1. As in Reliability Standard CIP-003-6, under proposed Reliability Standard CIP-003-7 entities are required to mitigate risks associated with routable communications by implementing controls to permit only necessary inbound and outbound electronic access to low impact BES Cyber Systems.

Protection of Transient Electronic Devices – As FERC recognized in Order No. 791, transient electronic devices are potential vehicles for cyber-attacks absent appropriate controls.[11] To that end, in Order No. 822, FERC (1) approved revisions to Reliability Standard CIP-010-2 to include mandatory protections for transient electronic devices, referred to as Transient Cyber Assets and Removable Media, used at high and medium impact BES Cyber Systems and (2) directed NERC to include mandatory protections for transient electronic devices used for a low impact BES Cyber Systems to improve the defense-in-depth approach of the CIP Reliability Standards.[12]

In response to this directive, NERC proposes additional revisions in Attachment 1 to CIP-003-7 to require entities to take steps to mitigate the risk to the BES related to malware propagation through the use of transient electronic devices at low impact BES Cyber Systems. Specifically, Attachment 1 is expanded to include a fifth section requiring entities to implement a plan to protect transient electronic devices to "achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems." The requirements in Section 5 of Attachment 1 are tailored to the risks posed by low impact BES Cyber systems and differentiate between Transient Cyber Assets and Removable Media and between Transient Cyber Assets managed by the Responsible Entity and Transient Cyber Assets managed by a party other than the Responsible Entity (e.g. vendors or contractors), as is the case in Reliability Standard CIP-010-2 for high and medium impact BES Cyber Systems. Additionally, NERC modified the definitions of Transient Cyber Asset and Removable Media to accommodate the use of the terms for all impact levels, as discussed below.

---

[11] Order No. 791 at PP 134-135.

[12] Order No. 822 at P 32.

CIP Exceptional Circumstance Policy – NERC also proposes revisions in Requirement R1 of proposed Reliability Standard CIP-003-7 to require Responsible Entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems, as is already required for high and medium impact BES Cyber Systems in CIP-003-6. As implementation of existing requirements applicable to low impact BES Cyber Systems is not subject to CIP Exceptional Circumstances, such a policy was not previously included in CIP-003-6 for low impact BES Cyber Systems. Because implementation of the proposed transient electronic device requirements applicable to low impact BES Cyber Systems in Section 5 of Attachment 1 to CIP-003-7 is subject to CIP Exceptional Circumstances, NERC proposes to require entities to have such a policy at this time.

For the reasons discussed herein, the proposed Reliability Standard is 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:

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

Howard Gugel
Senior Director, Standards and Education
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.[13] 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 of the 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 is required before NERC submits the Reliability Standard to the applicable governmental authorities.

B. Order No. 822 Directives

In Order No. 822, FERC approved revisions to seven CIP Reliability Standards to help improve the base-line cybersecurity posture of Responsible Entities. Among other things, the approved revisions, filed in response to FERC Order No. 791, included (1) enhanced security controls for low impact BES Cyber Systems related to cyber security awareness, physical security, electronic access control, and Cyber Security Incident response; and (2) mandatory protections for Transient Cyber Assets and Removable Media used for high and medium impact BES Cyber Systems.

In Order No. 822, FERC also directed NERC to develop the following modifications to improve the CIP Reliability Standards, among other things:

- Clarify the electronic access control requirements for low impact BES Cyber Systems by modifying the *NERC Glossary* definition for LERC to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 and eliminate ambiguity surrounding the term "direct" as it is used in the LERC definition.[14]

---

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

[14] Order No. 822 at P 73.

- Develop modifications to address the protection of transient electronic devices used at low impact BES Cyber Systems.[15]
- Develop modifications to protect communication links and sensitive BES data communicated between Control Centers.[16]

NERC was directed to file the modification related to LERC within one year of the effective date of Order No. 822, which is March 31, 2017. No deadline was set for filing modifications to address the other directives. This filing addresses modifications associated with the LERC and transient electronic device directives. NERC is currently developing modifications to the CIP Reliability Standards to address the directive related to communication links and sensitive BES data. Additional information on the LERC and transient electronic device directives is set forth below.

1. LERC Directive

As noted above, Reliability Standard CIP-003-6 requires Responsible Entities to implement electronic access controls to permit only necessary inbound and outbound access to low impact BES Cyber Systems for certain communications using routable protocol. Specifically, Section 3 of Attachment 1 to CIP-003-6 provides, in relevant part:

> **Section 3.** Electronic Access Controls: Each Responsible Entity shall:
>
> **3.1** For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and

The purpose of the LERC definition is to delineate the circumstances under which Responsible Entities are required to establish electronic access controls for low impact BES Cyber Systems that have bi-directional routable protocol communication with devices external to the

[15] *Id*. at P 32.

[16] *Id*. at P 53.

asset containing the low impact BES Cyber Systems. LERC is defined in the *NERC Glossary* as follows:

> Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bidirectional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

In FERC's Notice of Proposed Rulemaking ("NOPR") in Docket No. RM15-14-000, FERC requested comment on the clarity of the proposed LERC definition.[17] Specifically, FERC sought comment on: (1) the purpose of the meaning of the term "direct" in relation to the phrases "direct user-initiated interactive access" and "direct device-to-device connection" within the proposed definition; and (2) the implementation of the "layer 7 application layer break" contained in certain reference diagrams in the Guidelines and Technical Basis section of Reliability Standard CIP-003-6.[18]

In its NOPR Comments, NERC explained that the intent of the proposed LERC definition and Section 3 of Attachment 1 to CIP-003-6 was to require Responsible Entities to implement security controls (i.e., a LEAP) where no such controls or other barriers to electronic access would otherwise exist. As discussed in the Guidelines and Technical Basis section, the purpose of using the term "direct" in the LERC definition was to distinguish between the scenarios where an external user or device could electronically access the low impact BES Cyber System without a security break (i.e., "direct" access) from those situations where an external user or device could

---

[17] *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 152 FERC ¶ 61,054, at PP 69-70, 80 Fed. Reg. 43,354 (2015).

[18] NOPR at P 70.

only access the low impact BES Cyber System following a security break (i.e., "indirect" access).[19] The standard drafting team for Reliability Standard CIP-003-6 then designed the electronic access requirements for low impact BES Cyber Systems such that if an external user or device could connect to the low impact BES Cyber System without a security break, then the entity should implement a LEAP to control communication into either the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System. In contrast, if an external user or device could access the low impact BES Cyber System only following a security break, such that there were existing defenses to prevent connecting to the low impact BES Cyber System, then there is no need to implement a LEAP. Under either scenario, the standard drafting team concluded there would be sufficient barriers to accessing low impact BES Cyber Systems.[20]

NERC further explained, consistent with statements in the Guidelines and Technical Basis section, that LERC exists where communication from an external user or device flows through an intermediate Cyber Asset (e.g., an IP/Serial converter) and the intermediate Cyber Asset only does a "pass-through" of the communication (i.e., it does nothing more than extend the communication between the low impact BES Cyber System and the Cyber Asset external to the asset containing the low impact BES Cyber System). Only where the intermediate Cyber Asset provides a complete security break (i.e., prevents extending access to the low impact BES Cyber System from the external Cyber Asset) is there no LERC. In that scenario, NERC explained, there is no need to implement a LEAP as the security break provides sufficient protection commensurate to the risks presented by low impact BES Cyber Systems. The reference to the layer 7 application break in the

[19] NOPR Comments at 28-30.

[20] For instance, if the external user or device could connect to a low impact BES Cyber System only after going through another Cyber Asset, the user or device would have to know about that intermediate Cyber Asset and then figure out how to access the low impact BES Cyber System from the intermediate Cyber Asset, which provides a similar barrier to access that a LEAP is intended to provide.

Guidelines and Technical Basis section was used to demonstrate that if an entity implemented such a break to provide a complete security break, there would be no LERC.

In Order No. 822, FERC concluded that it is necessary to modify the LERC definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 so as to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition.[21] FERC fundamentally agreed with NERC that, as clarified in the Guidelines and Technical Basis section and NERC's pleadings, the construct established in CIP-003-6 provided sufficient electronic access protections for low impact BES Cyber Systems.[22]

2. Transient Electronic Device Directive

In Order No. 822, FERC approved revisions to Reliability Standards CIP-010-2 to include mandatory protections for Transient Cyber Assets and Removable Media used for high and medium impact BES Cyber Systems. FERC also directed NERC to include mandatory protections for transient electronic devices used for low impact BES Cyber Systems, concluding that it "will provide an important enhancement to the security posture of the BES by reinforcing the defense-in-depth nature of the CIP Reliability Standards at *all* impact levels."[23] FERC stated that "the modifications developed by NERC should be designed to effectively address the risks posed by transient electronic devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards."[24] FERC recognized that the protections for transient electronic devices used at low impact BES Cyber Systems "may be less

---

21 Order No. 822 at P 73.

22 Order No. 822 at P 75.

23 *Id*. at P 32.

24 *Id*. at P 32

stringent than the provisions that apply to medium and high impact BES Cyber Systems – commensurate with the risk."[25]

C. Development of the Proposed Reliability Standards

As further described in Exhibit G hereto, following the issuance of Order No. 822, NERC initiated a standard development project, Project 2016-02 Modifications to CIP Standards ("Project 2016-02"), to address the directives from Order No. 822 as well as issues identified during implementation of the CIP Reliability Standards approved in Order No. 791.

Given the filing deadline associated with the LERC directive, NERC prioritized development of revisions to address that directive. On July 21, 2016, NERC posted the initial draft of proposed Reliability Standard CIP-003-7 addressing only the LERC directive for a 45-day comment period and ballot. The initial ballot did not receive the requisite stakeholder approval. After considering comments to the initial draft, NERC posted a second draft of CIP-003-7 for another 45-day comment period and ballot on October 21, 2016. The second draft received the requisite stakeholder approval with an affirmative vote of 85.56%. NERC conducted a final ballot of this draft, which received an affirmative vote of 87.95%.

During the development of the second draft of CIP-003-7, the standard drafting team also began to develop language in response to the transient electronic device directive. On November 1, 2016, NERC posted draft revisions to CIP-003-7 to also address the transient electronic device directive for a 17-day informal comment period. On December 12, 2016, after considering comments received on the informal posting, NERC posted a third draft of CIP-003-7 that included the modifications to address the LERC directive, which had already received the requisite stakeholder approval, as well as modifications to address the transient electronic device directive

[25] *Id*. at P 35.

for a 45-day comment period and ballot.[26] This draft received the requisite stakeholder approval, with an affirmative vote of 81.30%. The final ballot for this draft of CIP-003-7, presented herein, received an affirmative stakeholder vote of 78.55%. The Board adopted proposed Reliability Standard CIP-003-7 on February 9, 2017.

IV. JUSTIFICATION

As discussed below and in Exhibit C, the proposed Reliability Standard satisfies the Reliability Standards criteria and is just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The following section provides an explanation of the manner in which the proposed Reliability Standard addresses the Order No. 822 directives related to electronic access and transient electronic devices for low impact BES Cyber Systems.

A. Electronic Access Controls for Low Impact BES Cyber Systems

As noted above, in response to FERC's directive to modify the LERC definition, NERC proposes to: (1) retire the *NERC Glossary* terms LERC and LEAP; and (2) modify Section 3 of Attachment 1 to Reliability Standard CIP-003-7 to more clearly delineate the circumstances under which Responsible Entities must establish electronic access controls for low impact BES Cyber Systems. The proposed retirement of LERC and LEAP and modifications to Section 3 of Attachment 1 are designed to simplify the electronic access control requirements for low impact BES Cyber Systems to avoid the ambiguities associated with the term "direct" and help ensure that Responsible Entities implement the required security controls effectively. NERC recognized that distinguishing between "direct" and "indirect" electronic access within the LERC definition

[26] During development, the third draft of CIP-003-7 was balloted as CIP-003-7(i). Romanette (i) was included in the version numbering to differentiate it from the earlier ballot of CIP-003-7 that only addressed the LERC directive.

added a layer of unnecessary complexity to identifying the circumstances under which entities must establish electronic access protection.

As discussed below, proposed Reliability Standard CIP-003-7 presents a straightforward approach, requiring Responsible Entities to implement electronic access controls for any communication, whether direct or indirect, between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System that use a routable protocol when entering or leaving the asset containing the low impact BES Cyber System. The proposed modifications to Section 3 of Attachment 1 improve the clarity of the electronic access requirements by untangling the type of communications requiring electronic access controls from whether controls are already in place to address that communication. The existence of a complete security break (i.e., indirect access) is simply treated as another form of electronic access control that is intended to meet the security objective. The proposed approach avoids overemphasis on identifying LERC and focuses Responsible Entities on the security objective of controlling electronic access to permit only necessary inbound and outbound electronic access to low impact BES Cyber Systems.

Proposed Section 3 of Attachment 1 to CIP-003-7 provides as follows:

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

The following is a discussion of each of the basic elements in Section 3 of Attachment 1 and the manner in which the proposed modifications improve the Reliability Standard. As NERC is not proposing any substantive modifications to Section 3.2 of Attachment 1 regarding Dial-up connectivity, the following discussion focuses on the modifications related to Section 3.1. As discussed below, there are three basic elements to Section 3.1: (1) identifying routable protocol communications from outside the asset containing the low impact BES Cyber System; (2) determining necessary inbound and outbound electronic access; and (3) implementing electronic access controls to permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Each of these elements is discussed below, in turn.

i. Identifying Routable Protocol Communications

As in Reliability Standard CIP-003-6, the initial step in determining whether a Responsible Entity must implement electronic access controls for its low impact BES Cyber systems under Section 3.1 of Attachment 1 to proposed CIP-003-7 is to identify whether there are any communications requiring electronic access controls. Whereas Reliability Standard CIP-003-6 references the LERC definition to define those communications, proposed Reliability Standard CIP-003-7 defines those circumstances within Section 3.1. Section 3.1 provides that communications with the following characteristics are subject to the electronic access control requirements, each of which had been included in the LERC definition:

(1) The communication is between the low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System.

(2) The communication uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System.

(3) The communication is not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

As NERC previously explained in discussing the LERC definition, the first characteristic helps to properly focus the electronic access controls.[27] Specifically, considering the wide array of low impact BES Cyber Systems and the risk-based approach to protecting different types of BES Cyber Systems, the requirement focuses the electronic access controls on communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System and not on inter-asset communication. From a risk perspective, controlling the accessibility to or from the asset containing the low impact BES Cyber System significantly reduces the scale of threats to low impact BES Cyber Systems.

As with the LERC definition, given the various types of assets containing low impact BES Cyber Systems, proposed Section 3.1 does not specify a bright line rule as to what constitutes communication from outside the asset. In demonstrating compliance with Section 3 of Attachment 1, Responsible Entities would be required to show the manner in which they identify external communications. Whether the Responsible Entity uses a logical border as a demarcation point or some other understanding of what is inside or outside the asset, it would have to provide a reasonable justification for its determination.

The second characteristic provides that the communication use a routable protocol when entering or leaving the asset because routable connections present increased risks to the security of the BES Cyber System and require additional protections. Whereas the LERC definition uses

[27] *Notice of Filing of the North American Electric Reliability Corporation of Proposed Critical Infrastructure 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 29, (Feb. 25, 2015).

the phrase "bi-directional routable protocol connection," proposed Section 3.1 uses the phrase "uses routable protocol when entering or leaving the asset." The modification recognizes that Responsible Entity's may use a uni-directional gateway to control electronic access. The intent, however, is the same. Namely, if communication with a low impact BES Cyber System involves routable connections to or from the asset containing the low impact BES Cyber System, the Responsible Entity must implement protections, such as a uni-directional gateway, to address the risk of uncontrolled communication.

As to the third characteristic, the exclusion of communications for time-sensitive protection or control functions between intelligent electronic devices was included in proposed Section 3.1, as in the LERC definition, so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future. The time-sensitive communications subject to the exclusion typically have communication delay allowances of less than 10 milliseconds. The standard drafting team was concerned that the introduction of the required access control processing would unacceptably impact the communications throughput in some cases. As explained in the Guidelines and Technical Basis section:

> Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles.

If a Responsible Entity invokes this exclusion, may have to demonstrate to the ERO that applying electronic access controls would introduce latency that would negatively impact functionality.

The language in proposed Reliability Standard CIP-003-7 for the exclusion is different from the language in the LERC definition but was not intended to substantially modify the exclusion. Specifically, NERC removed the reference to "Transmission stations" to allow for the exemption to apply to communications to a generation station and a control center, and modified the reference to "61850" to provide additional clarity.

As discussed above, the most significant difference between the LERC definition and the communications described in proposed Section 3.1 is that proposed Section 3.1 does not include "direct user-initiated interactive access or a direct device-to-device connection" as a characteristic for determining whether the communication is subject to electronic access controls. This modification does not change the electronic access control protections afforded to low impact BES Cyber Systems. Any communication, whether direct or indirect, using routable protocol from outside the asset is subject to the requirement to implement electronic access controls, unless the communication meets time-sensitive exclusion described above. Under proposed Reliability Standard CIP-003-7, implementing a security break would be a form of electronic access control that may be implemented to meet the objective of the requirement. By untangling the type of communications requiring electronic access controls from whether controls are already in place to address that communication, the proposed modifications establish a more straightforward approach that avoids confusion and helps promotes effective implementation.

ii. Determining Necessary Inbound and Outbound Electronic Access

As in Reliability Standard CIP-003-6, after identifying whether the communication is subject to electronic access controls, the next step is for Responsible Entities to determine whether to permit electronic access to or from the low impact BES Cyber System for the communication. Specifically, Section 3.1 provides that for communications subject to this requirement,

Responsible Entities may "permit only *necessary* inbound and outbound electronic access as determined by the Responsible Entity."

Considering the wide array of assets containing low impact BES Cyber Systems and the myriad of reasons a Responsible Entity may need to allow electronic access to or from a low impact BES Cyber System, Section 3.1 does not specify a bright line as to what constitutes "necessary inbound and outbound access." Entities have the flexibility to identify the necessary electronic access to meet their business and operational needs. To demonstrate compliance with Section 3.1, however, a Responsible Entity must document the necessity of its inbound and outbound electronic access permissions and provide justification of the need for such access.[28] Provided the Responsible Entity documents a reasonable business or operational need for the electronic access consistent with the security objective of the requirement, the ERO would not override the Responsible Entity's determination.[29] Absent a documented, reasonable justification for permitting electronic access, the ERO may find that the Responsible Entity was not compliant with Section 3.1.

During development of proposed Reliability Standard CIP-003-7, there were questions about the addition and meaning of the phrase "as determined by the Responsible Entity" in Section 3.1, as such language is not in Section 3.1 of CIP-003-6. In short, the purpose of the phrase is to

---

[28] As the standard drafting team stated in the Guidelines and Technical Bases section for CIP-003-7, "[h]owever the Responsible Entity chooses to document the inbound and outbound access permissions and the need, *the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted*." (Emphasis added)

[29] As such, the draft of the Reliability Standard Audit Worksheet ("RSAW") for CIP-003-7 provides as follows in the Note to Auditor section for Requirement R2: "The entity must document its determination as to what is necessary inbound and outbound electronic access and provide justification of the business need for such access. Once this determination has been made and documented, the audit team's professional judgment cannot override the determination made by the Responsible Entity." The draft RSAW is available at http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/RSAW_CIP-003-7(i)_v2_Clean_01202017.pdf.

indicate that the determination as to whether electronic access is necessary is to be made in the first instance by the Responsible Entity given the facts and circumstances of each case. The use of that phrase does not preclude the ERO from engaging in effective compliance oversight of the electronic access requirements in CIP-003-7. Specifically, when assessing compliance with Section 3.1, the ERO has the authority to review the Responsible Entity's documented justification for permitting the electronic access and to determine whether it is a reasonable exercise of the entity's discretion in light of the reliability objective of the requirement. As noted above, a failure to provide a reasonable justification may result in a finding of noncompliance.

The phrase "as determined by the Responsible Entity" or substantially similar language is used in 11 other instances in the CIP Reliability Standards, including Section 2 of Attachment 1 to Reliability Standard CIP-003-6, which provides:

> Each Responsible Entity shall control physical access, *based on need as determined by the Responsible Entity* [emphasis added], to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

In addition, the phrase "as determined by the Responsible Entity" or substantially similar language is used in the following instances in the CIP Reliability Standards: CIP-004-6, Requirement R4, Part 4.1; CIP-004-6, Requirement R4, Part 4.3; CIP-004-6, Requirement R4, Part 4.4; CIP-004-6, Requirement R4, Part 5.2; CIP-004-6, Requirement R4, Part 5.5; CIP-007-6, Requirement R1, Part 1.1; CIP-007-6, Requirement R1, Part 4.2; CIP-007-6, Requirement R4, Part 4.4; CIP-008-5, Requirement R3, Part 3.2; and CIP-009-6, Requirement R3, Part 3.2. Substantially similar language is also used in Reliability Standards IRO-002-4, Requirement R3; IRO-010-2, Requirement R1, Part 1.1; and TOP-003-3, Requirement R1, Part 1.1.

In each instance in which the "as determined by" or substantially similar language is used, the ERO has the authority to evaluate the reasonableness of the Responsible Entity's determination

when assessing compliance to ensure it is consistent with the reliability objective of the requirement. To interpret this language otherwise would be inconsistent with NERC's statutory obligation to engage in meaningful compliance oversight and the long-standing rule of statutory construction that requires courts to construe statutory language to avoid absurd results.[30]

For example, if the "as determined by" language in Section 2 of Attachment 1 to CIP-003-6 is interpreted to preclude the ERO from assessing the reasonableness of a Responsible Entity's determination as to whom to provide physical access to low impact BES Cyber Systems, a Responsible Entity could comply with the Reliability Standard even if it granted physical access to individuals based on the letter of the alphabet with which their last name begins. Implementing the requirement in this manner would be inconsistent with the security objective of the requirement, yet the ERO would have no authority to find the Responsible Entity noncompliant if it could not assess the reasonableness of the Responsible Entity's determination of need. Language in a Reliability Standard should not be read to allow for such a patently absurd result and limit the ERO's and the FERC's statutory authority to engage in meaningful compliance oversight and enforcement. Accordingly, when enforcing Sections 2 and 3 of Attachment 1 to CIP-003-7, as well as the other requirements that include the "as determined by" or substantially similar language, NERC would assess the reasonableness of the Responsible Entity's determination in light of the reliability and security objective in the requirement.

---

[30] *Mova Pharm. Corp. v. Shalala*, 140 F.3d 1060, 1068 (D.C. Cir. 1998); *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 59-61 (2007); *Lamie v. United States Trustee*, 540 U.S. 526, 533-534 (2004); *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 68-69 (1994); *United States v. Ron Pair Enters.*, 489 U.S. 235, 242 (1989); *United States ex rel. Totten v. Bombardier Corp.*, 380 F.3d 488, 494-95 (D.C. Cir. 2004). Moreover, even in absence of a plainly absurd result, courts construe statutes so as to further the statutory purpose. *K-Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 316 (1988); *Dolan v. Postal Service*, 546 U.S. 481, 486 (2006); *Cedar Rapids Cmty. Sch. Dist. v. Garret F.*, 526 U.S. 66, 73 (1999); *McCarthy v. Bronson*, 500 U.S. 136, 139 (1991); *Crandon v. United States*, 494 U.S. 152, 158 (1990); *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 571 (1982); RICHARD J. PIERCE, FEDERAL ADMINISTRATIVE LAW 567-69 (2010 ed.); Cass Sunstein, *Interpreting Statutes in the Regulatory State*, 103 HARV. L. REV. 405, 425-428 (1989).

iii. Implementation of Electronic Access Controls

The last element of Section 3.1 is to implement electronic access controls to permit only necessary electronic access to or from the low impact BES Cyber System. Whereas Reliability Standard CIP-003-6 references the LEAP definition, proposed CIP-003-7 replaces the reference to LEAP with a statement that Responsible Entities must "implement electronic access controls to permit only necessary inbound and outbound access…." The reference to LEAP was replaced because there are many different technical solutions that can be used to implement electronic access controls in addition to implementing a LEAP. The proposed modifications and the retirement of LEAP, however, do not fundamentally alter the security objective of, or the controls required by, Section 3 of Attachment 1. In short, once a Responsible Entity determines that there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System that uses a routable protocol when entering or leaving the asset, the Responsible Entity must implement an electronic access control to permit only necessary inbound and outbound electronic access.

As in Reliability Standard CIP-003-6, Responsible Entities have the flexibility under the proposed Reliability Standard to determine the controls necessary to meet this security objective. In the Guidelines and Technical Basis section, the standard drafting team provided conceptual illustrations of various electronic access controls that, if implemented effectively, may meet the security objective. Examples include, among other things:

- Implementation of a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is permitted to the low impact BES Cyber Asset.

- Use of a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber Asset, or to the network to which the low impact BES Cyber Asset is connected.

- Use of a non-BES Cyber Asset that requires authentication for communication from Cyber Assets outside the asset containing the low impact BES Cyber System before allowing the connection to the low impact BES Cyber Asset to be established.

- Physical or logical isolation of the low impact BES Cyber System from other communications.

In assessing compliance with Section 3 of Attachment 1 to proposed Reliability Standard CIP-003-7, the ERO would evaluate the manner in which the Responsible Entity implemented its electronic access controls to determine whether it meets the security objective.

Lastly, with the proposed retirement of the LEAP definition, NERC is also proposing modifications to Section 2 of Attachment 1 (physical security controls) to replace references to LEAP with the more generic phrase "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." This proposed modification does not substantively modify the obligation from CIP-003-6 to implement physical access controls for those Cyber Assets that control electronic access to low impact BES Cyber Systems.

B. Protection of Transient Electronic Devices Used for Low Impact BES Cyber Systems

Consistent with FERC's directive in Order No. 822, proposed Reliability Standard CIP-003-7 includes mandatory protections for transient electronic devices used at low impact BES Cyber Systems. Specifically, NERC proposes to add a fifth section to Attachment 1 to CIP-003-7 to require entities to include in their cyber security plans controls to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. Proposed Section 5 of Attachment 1 provides as follows:

> **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 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.

5.3 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.

Requiring the Responsible Entity to develop and implement these controls will provide enhanced protections against the propagation of malware from transient electronic devices.

The language in proposed Section 5 parallels the language in Attachment 1 to Reliability Standard CIP-010-2 related to mitigating the risks of the introduction of malicious code to high and medium impact BES Cyber Systems through the use of Transient Cyber Assets and

Removable Media. As in Reliability Standard CIP-010-2, proposed Section 5 of Attachment 1 to CIP-003-7 distinguishes between Transient Cyber Assets and Removable Media and between Transient Cyber Assets managed by the Responsible Entity and those managed by a party other than the Responsible Entity. The security controls required for a particular transient electronic device must account for the functionality of that device and, for Transient Cyber Assets, whether the Responsible Entity or another party manages the device. Because Transient Cyber Assets and Removable Media have different capabilities, they present different levels of risk to the BES, and the protections required under the proposed Reliability Standards must reflect those differences. Similarly, because a Responsible Entity lacks complete control over Transient Cyber Assets managed by a third party, it may not be able to implement the same controls for those devices as it does for the devices it manages. The Responsible Entity, however, still has the responsibility to mitigate the risks associated with Transient Cyber Assets managed by a third party prior to connection.[31]

Further, as in Reliability Standard CIP-010-2, proposed Section 5 of Attachment 1 does not prescribe a standard method or set of controls that each Responsible Entity must implement to protect its transient electronic devices. Instead, Section 5 requires Responsible Entities to meet certain security objectives by implementing the controls that the Responsible Entity determines necessary to meet its affirmative obligation to mitigate the risks of the introduction of malicious code. This approach provides the Responsible Entity the flexibility to implement the controls that best suit the needs and characteristics of its organization. To comply with the requirements in

[31] Given the functionality of Removable Media, the standard drafting team concluded that it was not necessary to distinguish between Removable Media managed by the responsible entity and those managed by a third party. That is because, no matter who manages Removable Media, the same type of security controls can be applied (e.g., the scanning of a thumb drive prior to connection).

Section 5, however, the Responsible Entity must demonstrate that its selected controls were designed to meet the security objective to mitigate the risk of the introduction of malicious code.

In contrast to Attachment 1 of Reliability Standard CIP-010-2, Section 5 of Attachment 1 to CIP-003-7 does not include requirements related to authorization or software vulnerabilities. Consistent with the risk-based approach of the CIP Reliability Standards and the underlying principle of concentrating limited industry resources on protecting those BES Cyber Systems with greater risks to the BES, proposed Section 5 focuses directly on the primary risk associated with the use of Transient Cyber Assets and Removable Media, which is the introduction of malicious code. The protections required in proposed Section 5 are commensurate to the cybersecurity risk of low impact BES Cyber Systems and would not divert Responsible Entities' focus from the protection of high and medium impact BES Cyber Systems. As FERC recognized in Order No. 791, the requirements applicable to low impact BES Cyber Systems, given their lower risk profile, should not be overly burdensome to divert resources from the protection of medium and high impact BES Cyber Systems.[32]

Further, as compared to the requirements in Attachment 1 to CIP-010-2, proposed Section 5 of Attachment 1 to CIP-003-7 does not include language explicitly stating that for the method(s) used to mitigate the introduction of malicious code from Transient Cyber Assets managed by a party other than the Responsible Entity, the Responsible Entity shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Assets. Nevertheless, NERC's expectation is that if another party's processes and practices for protecting its Transient Cyber Assets do not provide reasonable assurance that they

[32] Order No. 791 at P 111 (finding that it would be unduly burdensome to require responsible entities to create and maintain an inventory of Low Impact assets for audit purposes).

are designed to effectively meet the security objective of mitigating the introduction of malicious code, the Responsible Entity must take additional steps to meet the stated objective. In assessing compliance with the proposed Reliability Standard, NERC will focus on whether the Responsible Entity implemented one or more controls designed to achieve the security objective. Accordingly, if a Responsible Entity reviews the policies and practices of another party and those practices and policies do not provide reasonable assurance that the party's transient electronic devices would be protected from malicious code, simply reviewing those policies and procedures without taking other steps to mitigate the risks of introduction of malicious code may not constitute compliance.

In addition to the modifications in Attachment 1 to CIP-003-7, NERC also proposes modifications to the definitions of Transient Cyber Asset and Removable Media to accommodate the use of those terms for all impact levels. As those definitions were originally drafted for use of transient electronic devices at high and medium impact BES Cyber Systems only, they include references to other *NERC Glossary* terms – Electronic Security Perimeter and Protected Cyber Asset – that specifically relate to concepts or requirements associated with high and medium impact BES Cyber Systems only. So as to avoid confusion as to the application of Electronic Security Perimeters and Protected Cyber Assets at low impact BES Cyber Systems, the definitions of Transient Cyber Asset and Removable Media were modified.

As provided in Exhibit B hereto, the proposed definition for Transient Cyber Asset is as follows:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and

4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:

   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Similarly, the proposed definition for Removable Media is as follows:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:

   - BES Cyber Asset, ~~a~~
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or ~~a~~
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

C. CIP Exceptional Circumstance Policy

NERC also proposes revisions in Requirement R1 of CIP-003-7 to require Responsible Entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems, as is already required for their high and medium impact BES Cyber Systems. As defined in the *NERC Glossary*, a CIP Exceptional Circumstance is:

> A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

In the existing CIP Reliability Standards, a number of requirements applicable to high and medium impact BES Cyber Systems specify that Responsible Entities need not implement (or continue implementing) the requirement during CIP Exceptional Circumstances.[33] The purpose of this exception is not to require implementation when the Responsible Entity would be physically unable to implement due to the CIP Exceptional Circumstance or implementation would hinder the Responsible Entity's ability to timely and effectively respond to the CIP Exceptional Circumstance. To that end, under Reliability Standard CIP-003-6, Requirement R1, Part 1.1, a Responsible Entity must have cyber security policies for its high and medium impact BES Cyber System that addresses, among other topics, declaring and responding to CIP Exceptional Circumstances. These policies would outline the procedures Responsible Entities would take to address a CIP Exceptional Circumstance in the context of its cyber security requirements.

As the existing requirements in CIP-003-6 applicable to low impact BES Cyber Systems are not subject to CIP Exceptional Circumstances, such a policy was not included in CIP-003-6, Requirement R1, Part 1.2 for low impact BES Cyber Systems. Now that the proposed requirements related to transient electronic devices used at low impact BES Cyber Systems include an exception for CIP Exceptional Circumstances,[34] NERC is proposing to add a new part to Requirement R1 of

---

[33] *See*, *e.g.*, CIP-004-6, Requirement R2, Part 2.2; CIP-004-6, Requirement R4, Part 4.1; CIP-006-6, Requirement R2, Part 2.1.

[34] The requirements applicable to the protection of transient electronic devices at high and medium impact BES Cyber Systems also includes an exception for CIP Exceptional Circumstances. *See* CIP-010-2, Requirement R4.

CIP-003-7, Part 1.2.6, to require entities to have a CIP Exceptional Circumstance policy applicable to low impact BES Cyber Systems.

V. EFFECTIVE DATE

Proposed Reliability Standard CIP-003-7 and the revised definitions of Transient Cyber Asset and Removable Media will become effective as set forth in the proposed Implementation Plan, provided in Exhibit C hereto. The proposed Implementation Plan provides that, where approval by an applicable governmental authority is required, Reliability Standard CIP-003- 7 shall become effective on the first day of the first calendar quarter that is eighteen (18) 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- 003-7 shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction. For the revised definitions of Transient Cyber Asset and Removable Media, where approval by an applicable governmental authority is required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the definitions, or as otherwise provided for by the applicable governmental authority. Where approval by an applicable governmental authority is not required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date that the definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction. The 18-month implementation period is designed to

afford Responsible Entities sufficient time to revise their cyber security plans for low impact BES Cyber Systems under proposed Reliability Standard CIP-003-7, Requirement R2 to account for the proposed modifications and implement the required controls.

Additionally, as entities must implement the current version of Sections 2 and 3 of Attachment 1 to Reliability Standard CIP-003-6 on September 1, 2018, the proposed Implementation Plan provides that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of proposed Reliability Standard CIP-003-7. This provision is to avoid the situation where Responsible Entities would have to have their cyber security plans and implement electronic access protections using the LERC and LEAP construct and then a short time later modify those plans to account for the changes proposed herein.

Lastly, the Implementation Plan provides that Reliability Standard CIP-003-6 and the current definitions of LERC, LEAP, Removable Media, and Transient Cyber Asset shall be retired immediately prior to the effective date of proposed Reliability Standard CIP-003-7.

Respectfully submitted,

/s/ Shamai Elstein

Shamai Elstein
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net
Marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: March 10, 2017

EXHIBITS A-C and E-H

EXHIBIT D

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 purpose of proposed Reliability Standard CIP-003-7 is to specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk-Electric System. The modifications in the proposed Reliability Standard achieve the specific reliability goal of improving upon the existing protections applicable to low impact BES Cyber Systems by: (1) clarifying the electronic access control requirements applicable to low impact BES Cyber Systems; (2) adding requirements related to the protection of transient device transient electronic devices used for low impact BES Cyber Systems; and (3) requiring Responsible Entities to have a documented cyber security policy related to declaring and responding to CIP Exceptional Circumstances for low impact BES Cyber Systems, consistent with the FERC directives in Order No. 822. The proposed revised definitions for Transient Cyber Asset ("TCA") and Removable Media ensure the applicability of those terms for all impact levels: high, medium and low. The revisions to the proposed definitions allow entities to deploy one program to manage TCAs and Removable Media across multiple impact levels.

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,

Distribution Providers, Generator Operators, Generator Owners, Interchange Coordinators or Interchange Authorities, 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 ("VRFs") 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 F**. 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, proposed Reliability Standard CIP-003-7 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 Standard contains Measures that support each Requirement by clearly identifying what is required and how the Requirements will be measured for compliance. The Measures are listed after each of the Requirements of proposed CIP-003-7 and provide clarity on types of evidence to support each Requirement, which will allow the Requirements to be enforced in a consistent and non-preferential manner. The Measures are provided within the proposed Reliability Standard in **Exhibit A**.

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 modifications to the proposed Reliability Standard clearly articulate the security objectives that applicable entities must implement, including (1) electronic access controls for any communication, whether direct or indirect, between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System that use a routable protocol when entering or leaving the asset containing the low impact BES Cyber System, and (2) protections for transient electronic devices used for low impact 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. To the contrary, the proposed Reliability Standard contains significant benefits for the Bulk-Power System. The requirements of the proposed Reliability Standard help ensure that entities mitigate risks associated with routable communications to low impact BES Cyber Systems and the use of transient electronic devices for low impact BES Cyber Systems.

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 and revised definitions 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.**

Proposed Reliability Standard CIP-003-7 will not cause undue negative effect on competition or result in any unnecessary restrictions.

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

The proposed effective date for proposed Reliability Standard CIP-003-7 and the proposed revised definitions of "Transient Cyber Asset" and "Removable Media" is just and reasonable. NERC proposes an effective date as provided in the Implementation Plan. The proposed implementation period is designed to allow sufficient time for the applicable entities to

make any changes in their internal process necessary to implement proposed CIP-003-7. The proposed Implementation Plan is attached as **Exhibit C**.

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 and revised definitions was developed in accordance with NERC's ANSI- accredited processes for developing and approving Reliability Standards.[1] **Exhibit G** includes a summary of the Reliability Standard development proceedings, and details the processes followed to develop the Reliability Standard and revised Definitions. These processes included, among other things, comment and balloting periods. Additionally, all meetings of the drafting team were properly noticed and open to the public.

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 proposed Reliability Standard CIP-003-7 and revised definitions of "Transient Cyber Asset" and "Removable Media". No comments were received that indicated the proposed Reliability Standard or revised definitions 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 CIP-003-7 is just and reasonable were identified.

---

[1] *See* NERC Rules of Procedure, Section 300 (Reliability Standards Development) and Appendix 3A (Standard Processes Manual).