UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls	)))	Docket No. RM17-11-000

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") provides comments on the Federal Energy Regulatory Commission's ("FERC" or the "Commission") Notice of Proposed Rulemaking ("NOPR") proposing to approve Critical Infrastructure Protection ("CIP") Reliability Standard CIP-003-7 (Cyber Security – Security Management Controls).[1] NERC supports the Commission's proposal to approve the proposed Reliability Standard. As discussed in the NOPR, proposed Reliability Standard CIP-003-7 improves upon the currently-effective CIP Reliability Standards by: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; (2) adopting mandatory security controls for transient electronic devices used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems.[2]

In the NOPR, the Commission also proposes "to direct that NERC modify Reliability Standard CIP-003-7 to: (1) provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems; and (2) address the need to mitigate the risk of malicious code that

[1] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 161 FERC ¶ 61,047 (2017).

[2] NOPR at P 2.

could result from third-party transient electronic devices."[3] As discussed below, the proposed directives may not be necessary to address potential security gaps or improve the cyber security posture of responsible entities. Nevertheless, NERC does not oppose further evaluation of ways to improve the clarity and auditability of the requirements in Reliability Standard CIP-003-7 through its standard development process, consistent with the Commission's proposed directives.

The following is a discussion of each of the proposed directives.

I. Electronic Access Controls for Low Impact BES Cyber Systems

Section 3.1 of Attachment 1 to proposed Reliability Standard CIP-003-7 is designed to reduce risks associated with uncontrolled communications to low impact BES Cyber Systems. Proposed Reliability Standard CIP-003-7 requires Responsible Entities to implement electronic access controls to permit only necessary inbound and outbound electronic access to low impact BES Cyber Systems. The electronic access controls must be applied to routable communications between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System. As discussed in NERC's Petition, the modifications in Section 3.1 improve the electronic access control requirements for low impact BES Cyber systems by more clearly delineating the circumstances under which Responsible Entities must establish those electronic access controls.[4]

In the NOPR, however, the Commission expressed concern regarding the auditability of Section 3.1. The Commission stated:

> Proposed Reliability Standard CIP-003-7 does not provide clear, objective criteria or measures to assess compliance by independently confirming that the access control strategy adopted by a responsible entity would reasonably meet the security

[3] NOPR at 3.

[4] *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-003-7* at 16-26, Docket No. RM17-11-000 (Mar. 3, 2017) ("Petition").

objective of permitting only 'necessary inbound and outbound electronic access' to its low impact BES Cyber Systems.[5]

The Commission asserts that the standard should require the Responsible Entity to (1) articulate in its plan its access control strategy for a particular set of low impact BES Cyber Systems and provide a technical rationale rooted in security principles explaining how that strategy will reasonably restrict electronic access; and (2) outline basic security principles in order to provide clear, objective criteria or measures to assist in assessing compliance.[6] The Commission maintains that, without such requirements, "auditors will not necessarily have adequate information to assess the reasonableness of the responsible entity's decision with respect to how the responsible entity identified necessary communications or restricted electronic access to specific low impact BES Cyber Systems."[7]

NERC appreciates the Commission's concerns regarding auditability. The additional provisions proposed by the Commission, however, may not be necessary. As discussed in the Petition, Responsible Entities must provide auditors sufficient information to allow the auditor to properly assess compliance with Section 3.1.[8] Section 3.1 articulates a clear security objective: permit only necessary inbound and outbound access to low impact BES Cyber Systems. Considering the wide array of low impact BES Cyber Systems and their lower risk to Bulk Electric System reliability, Section 3.1 is not prescriptive. Responsible Entities have the flexibility to identify the necessary inbound and outbound access permissions and the appropriate electronic access controls. To comply with Section 3.1, however, a Responsible Entity must demonstrate that

---

5 NOPR at P 28.

6 NOPR at P 29.

7 *Id.*

8 *See* Petition at 21-24.

its electronic access permissions and controls are consistent with the security objective. The Responsible Entity must document the necessity of its inbound and outbound electronic access permissions and provide justification of the need for such access.[9] During compliance monitoring activities, NERC and the Regional Entities (collectively, the "ERO Enterprise") would review the Responsible Entity's documented justification to determine whether it is a reasonable exercise of the entity's discretion in light of the security objective of the requirement. If the Responsible Entity fails to articulate a reasonable business or operational need for the electronic access permission, the ERO Enterprise would find that the Responsible Entity did not comply with Section 3.1.

The Responsible Entity must also demonstrate that it implemented electronic access controls reasonably designed to restrict electronic access to the necessary communications. Consistent with the intent of the Commission's proposed directive, the Responsible Entity would have to articulate its access control strategy for the low impact BES Cyber System and provide a technical rationale rooted in security principles, explaining how that strategy will reasonably restrict electronic access. During compliance monitoring activities, the ERO Enterprise would review the Responsible Entity's implementation to determine whether the implemented controls meet the security objective. For instance, if a Responsible Entity uses a host-based firewall technology to manage inbound and outbound electronic access permissions to the low impact BES Cyber Systems, the ERO Enterprise would review the manner in which that technology is configured and deployed. If the Responsible Entity fails to demonstrate that its chosen electronic access controls are properly designed and implemented to meet the security objective, the ERO Enterprise would find that the Responsible Entity did not comply with Section 3.1.

[9] Petition at 22.

For these reasons, the proposed directive may not be necessary and may be an inefficient use of NERC and industry resources. Nevertheless, NERC does not oppose further evaluation of ways to improve the clarity and auditability of the requirements in Reliability Standard CIP-003-7 through its standard development process, consistent with the Commission's proposed directives. Articulating objective criteria for electronic access controls for low impact BES Cyber Systems within Section 3.1 may improve clarity and auditability, and help ensure that entities implement effective electronic access controls.

II. Protection of Transient Electronic Devices

As discussed in the Petition, Section 5 of Attachment 1 to proposed Reliability Standard CIP-003-7 requires entities to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of transient devices (i.e., Transient Cyber Assets and Removable Media).[10] Proposed Section 5 includes requirements related to Transient Cyber Assets owned/managed by the Responsible Entity and those owned/managed by third parties. For Transient Cyber Assets owned by third parties, Responsible Entities must use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System: (1) review of antivirus update level; (2) review of antivirus update process used by the party; (3) review of application whitelisting used by the party; (4) review use of live operating system and software executable only from read-only media; (5) review of system hardening used by the party; or (6) other method(s) to mitigate the introduction of malicious code.[11]

In the NOPR, the Commission proposed to direct NERC to develop modifications to proposed Reliability Standard CIP-003-7 to address the need to mitigate the risk of malicious code

[10] Petition at 26-31.

[11] *See* Petition at 27.

that could result from third-party Transient Cyber Assets. The Commission stated that "proposed Reliability Standard CIP-003-7 does not explicitly require mitigation of the introduction of malicious code from third-party managed Transient Cyber Assets, even if the responsible entity determines that the third-party's policies and procedures are inadequate."[12] FERC is concerned that without an explicit requirement for entities to determine whether any additional actions are necessary prior to connecting third-party devices to low impact BES Cyber Systems, an entity "could, without compliance consequences, simply accept the risk of deficient third-party transient electronic device management practices."[13]

As stated in the petition, NERC agrees with the Commission that, should a Responsible Entity find that a third party's processes and practices for protecting its transient electronic devices inadequate, the Responsible Entity must be required to take mitigating action prior to connecting third-party transient electronic devices to a low impact BES Cyber System.[14] NERC explained that, under proposed Reliability Standard CIP-003-7, failure to take mitigating action in this circumstances could result in a finding of noncompliance with Section 5 of Attachment 1.[15] Accordingly, the proposed directive may not be necessary and may be an inefficient use of NERC and industry resources. Nevertheless, NERC does not oppose further evaluation of ways to improve the clarity and auditability of Section 5 through its standard development process, consistent with the Commission's proposed directives. Modifying proposed Section 5 to explicitly include a mitigation requirement for third-part devices may remove any doubt about compliance expectations.

---

12 NOPR at P 39.

13 NOPR at P 40.

14 Petition at 29.

15 Petition at 29-30.

III. Conclusion

NERC respectfully requests that the Commission consider these comments and approve proposed Reliability Standard CIP-003-7.

Respectfully submitted,

/s/ Shamai Elstein

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

Counsel for the North American Electric Reliability Corporation

Date: December 22, 2017