NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 4, 2018

VIA ELECTRONIC FILING

Kirsten Walli, Board Secretary
Ontario Energy Board
P.O Box 2319
2300 Yonge Street
Toronto, Ontario, Canada
M4P 1E4

Re: *North American Electric Reliability Corporation*

Dear Ms. Walli:

The North American Electric Reliability Corporation hereby submits Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-012-1. 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

ONTARIO ENERGY BOARD
OF THE PROVINCE OF ONTARIO

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

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-012-1

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

October 4, 2018

TABLE OF CONTENTS

ONTARIO ENERGY BOARD
OF THE PROVINCE OF ONTARIO

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION)
)

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-012-1

The North American Electric Reliability Corporation ("NERC") hereby submits for approval proposed Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers. The proposed Reliability Standard addresses the Federal Energy Regulatory Commission's ("FERC") directive from Order No. 822[1] to modify the Critical Infrastructure Protection ("CIP") Reliability Standards to require Responsible Entities[2] to implement controls to protect communication links and sensitive Bulk Electric System ("BES") data communicated between BES Control Centers.[3] The proposed Reliability Standard, provided in Exhibit A hereto, is just, reasonable, not unduly discriminatory or preferential, and in the public interest. NERC also requests approval of the associated Implementation Plan (Exhibit B) and the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibit G).

This Petition presents the technical basis and purpose of the proposed Reliability Standard, a summary of the development history (Exhibit H), and a demonstration that the proposed

---

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

[2] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entities subject to the CIP Reliability Standards.

[3] 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.

Reliability Standard meets the Reliability Standards criteria (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standard on August 16, 2018.

I. EXECUTIVE SUMMARY

The proposed Reliability Standard improves upon and expands the protections required by NERC's CIP Reliability Standards by requiring Responsible Entities to protect the confidentiality and integrity of sensitive data pertaining to Real-time operations while being transmitted between BES Control Centers. As Responsible Entities use this sensitive data to operate and monitor the system in Real-time, it is critical for BES reliability that the data is accurate and secure. NERC developed proposed Reliability Standard CIP-012-1 in response to FERC's directive in Order No. 822 to develop modifications to Reliability Standard CIP-006-6 to require Responsible Entities to implement controls to protect communication links and sensitive BES data communicated between BES Control Centers. Rather than revise CIP-006-6, NERC determined that a new Reliability Standard was appropriate given the differences in applicability and scope between CIP-006-6 and proposed CIP-012-1.

Proposed Reliability Standard CIP-012-1 requires Responsible Entities to develop a plan to mitigate the risks posed by unauthorized modification (integrity) and unauthorized disclosure (confidentiality) of Real-time Assessment and Real-time monitoring data. The plan must include the following three components: (1) identification of security protection used to meet the security objective; (2) identification of where the Responsible Entity applied the security protection; and (3) identification of the responsibilities of each Responsible Entity for applying the security protection, if the communicating Control Centers are owned by different entities. Consistent with FERC's directive, proposed CIP-012-1 supports reliable operation of the BES as protecting the integrity and confidentiality of Real-time Assessment and Real-time monitoring data helps

maintain situational awareness and reliable BES operations through timely and accurate communication between Control Centers.

Consistent with the directive in Order No. 822, NERC considered the risks posed by different types of BES Control Centers and the data communicated between those Control Centers to determine the scope and applicability of the proposed standard. Proposed Reliability Standard CIP-012-1 applies to all Responsible Entities who own or operate Control Centers, with one limited exemption. As explained in greater detail below, the exemption applies to facilities that, while meeting the definition of Control Center, only communicate Real-time data with other Control Centers regarding a co-located field asset – i.e., a transmission station or generation facility. The Standard Drafting Team ("SDT") for the proposed standard determined that such Control Center communications are more akin to communications from a field asset such that a compromise of such communications does not pose a heightened risk to reliability in the same manner as the communication of aggregated Real-time Assessment and Real-time monitoring data between Control Centers. As such, consistent with FERC's exclusion of field asset communications from the directive in Order No. 822, NERC determined that Responsible Entities should focus resources on protecting aggregated Real-time Assessment and Real-time monitoring data exchanged between Control Centers, not data from Control Centers that only communicate data about a specific field asset. In addition, oral communications are not required to be protected under proposed CIP-012-1 because that method of communication does not present the same vulnerabilities, as discussed more fully below.

The proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The proposed Reliability Standard is to become effective as set forth in the proposed Implementation Plan.

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

The following background information is provided below: (a) a description of the NERC Reliability Standards Development Procedure; (b) an overview of the Order No. 822 directive addressed in this Petition; and (c) the history of the Project 2016-02 Modifications to CIP Standards SDT work on proposed Reliability Standard CIP-012-1.

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.[4] NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfy certain criteria for approving

[4] 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.

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. 822 Directive

In Order No. 822, FERC directed NERC to develop modifications to Reliability Standard CIP-006-6 to require protections for communication network components and data communicated between all BES Control Centers according to the risk posed to the BES.[5] In light of the critical role Control Center communications play in maintaining BES reliability, the directive focused on communications between Control Centers, not between a Control Center and non-Control Center facilities, such as Transmission substations or generation facilities.[6] FERC agreed with NERC and other commenters that "inter-Control Center communications play a critical role in maintaining [BES] reliability by, among other things, helping to maintain situational awareness and reliable [BES] operations through timely and accurate communication between Control Centers."[7]

FERC stated that in response to the directive, NERC should identify the scope of sensitive BES data that must be protected and specify how the confidentiality, integrity, and availability of each type of BES data should be protected while it is being transmitted or at rest.[8] As an example for the type of data to be protected, FERC highlighted the data specified by the Interconnection Reliability Operations and Coordination ("IRO") and Transmission Operations ("TOP") Reliability Standards. Specifically, FERC cited Reliability Standard TOP-003-3, Requirements

---

5 Order No. 822 at P 3.

6 *Id*. at P 41 (citing *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 152 FERC ¶ 61,054, at P 59 (2015) ("Notice of Proposed Rulemaking").

7 *Id*. at P 54.

8 *Id*. at P 56.

R1, R3, and R5, in which a "[T]ransmission [O]perator must maintain a documented specification for data and distribute its data specification to entities that have data required by the [T]ransmission [O]perator's Operational Planning Analyses, Real-time [m]onitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification."[9]

C. Development of the Proposed Reliability Standard

As further described in Exhibit H hereto, following the issuance of Order No. 822, NERC initiated a Reliability Standard development project, Project 2016-02 Modifications to CIP Standards ("Project 2016-02"), to address the directives from Order No. 822 and other revisions to the currently-effective CIP Reliability Standards. On July 27, 2017, NERC posted the initial draft of proposed Reliability Standard CIP-012-1 for a 45-day comment period and ballot. The initial ballot did not receive the requisite approval from the registered ballot body ("RBB"). After considering comments to the initial draft, NERC posted a second draft of CIP-012-1 for another 45-day comment period and ballot on October 27, 2017, which also failed to receive the requisite approval from the RBB. On March 16, 2018, NERC posted a third draft of proposed Reliability Standard CIP-012-1 for another 45-day comment period and ballot. Although the third draft received the requisite approval from the RBB, the Project 2016-02 SDT determined to make substantive revisions to CIP-012-1 to address commenter concerns. On May 18, 2018, NERC posted a fourth draft of proposed Reliability Standard CIP-012-1 for another 45-day comment period and ballot. The fourth draft of proposed Reliability Standard CIP-012-1 received the requisite approval from the RBB with affirmative votes of 68.45 percent of the ballot pool. NERC conducted a 10-day final ballot for proposed Reliability Standard CIP-012-1, which received

[9] *Id*. P 54 n.61.

affirmative votes of 72.55 percent of the ballot pool. The Board adopted the proposed Reliability Standard on August 16, 2018.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standard addresses FERC's directive in Order No. 822 and is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The following section provides an explanation of:

- the purpose and overview of the proposed Reliability Standard (Subsection A);
- the scope and applicability of the proposed Reliability Standard (Subsection B);
- the requirement in proposed Reliability Standard CIP-012-1, including a discussion of the manner in which it addresses the directive in Order No. 822 (Subsection C);[10] and
- the enforceability of the proposed Reliability Standard (Subsection D).

A. Purpose and Overview of the Proposed Reliability Standard

The purpose of the proposed Reliability Standard is to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers. In requiring protections of this data, proposed CIP-012-1 helps maintain situational awareness and reliable BES operations. In order for certain Responsible Entities to adequately perform their Real-time reliability functions, their associated Control Centers must be capable of receiving and storing a variety of sensitive BES data from interconnected entities. Helping to ensure the timeliness and accuracy of these communications through the proposed protections in CIP-012-1 would thus support reliable operations of the BES.

The SDT determined to address FERC's directive by developing a new standard, proposed Reliability Standard CIP-012-1, rather than revising Reliability Standard CIP-006-6 due to the differences in scope and applicability. Whereas CIP-006-6, Requirement R1, Part 1.10 requires

[10] Proposed Reliability Standard CIP-012-1 consists of one requirement with three parts.

protections for nonprogrammable communication components outside of a Physical Security Perimeter ("PSP") but inside the same Electronic Security Perimeter ("ESP") for certain Cyber Assets, proposed CIP-012-1 requires protections for communications between Control Centers that transmit certain data regardless of the location of Cyber Assets inside or outside a PSP or ESP. Moreover, the applicability of protections included in proposed CIP-012-1 differs from that of CIP-006-6. Proposed CIP-012-1 does not apply to BES Cyber Systems. Whereas CIP-006-6, Requirement R1, Part 1.10 applies to high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers, proposed CIP-012-1 applies to communications between certain Control Centers. As a result of these differences, the SDT determined that FERC's directive would best be met by developing a new Reliability Standard instead of revising CIP-006-6.

As discussed further below, proposed Reliability Standard CIP-012-1 requires Responsible Entities to develop and implement a plan to address the risks posed by unauthorized disclosure (confidentiality) and unauthorized modification (integrity) of Real-time Assessment and Real-time monitoring data while being transmitted between applicable Control Centers. The plan must include the following: (1) identification of security protections; (2) identification of where the protections are applied; and (3) identification of the responsibilities of each entity if the Control Centers are owned or operated by different Responsible Entities.

B. Applicability and Scope of the Proposed Reliability Standard

1) Applicable Functional Entities and Facilities

Proposed CIP-012-1 applies to entities registered as Balancing Authorities, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners that own or operate a Control Center as defined in the *Glossary of Terms Used in NERC Reliability Standards*. The proposed standard applies to Control Centers with high, medium, and low impact BES Cyber Systems. Proposed CIP-012-1 focuses on Responsible

Entities that own or operate Control Centers, regardless of the impact level of BES Cyber Systems located at or associated with those Control Centers. The SDT determined that the sensitivity of Real-time data communicated between Control Centers is not necessarily dependent on the impact level of the BES Cyber Systems located at or associated with the Control Centers.

In reviewing the types of Control Centers that should be subject to proposed CIP-012-1, the SDT instead focused on the types of Real-time data a Control Center would send, and whether, if the data were to be compromised, it would pose a high risk to the reliability of the BES. As FERC recognized, "not all communication network components and data pose the same risk to [BES] reliability and may not require the same level of protection."[11]

In conducting its analysis, the SDT determined that a limited subset of Control Centers should not be subject to the requirements in proposed CIP-012-1 given the limited data they transmit to other Control Centers. Specifically, as provided in the applicability section of proposed CIP-012-1, the following Control Centers are exempt from the proposed standard:

> A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.

The manner in which these Control Centers communicate with other Control Centers is no different from the manner in which a field asset (e.g., generating resources or Transmission substations) would communicate with a Control Center. In contrast to the Control Centers subject to proposed CIP-012-1, which exchange aggregated Real-time data, the Control Centers subject to the proposed exemption only send data regarding the status of a co-located field asset, like remote terminal unit data. If such data were compromised, the risk to the BES is lower than data from

---

[11] Order No. 822 at P 56.

those Control Centers transmitting data on multiple units. As discussed above, FERC's directive is not focused on the exchange of data between field assets and Control Centers.[12] FERC specifically rejected the argument to apply the directive to communications between all facilities of the BES, such as substations, stating that "the record in the immediate proceeding does not support such a broad requirement at this time."[13]

As discussed in more detail in the next subsection, the type of data transmitted between Control Centers that is within the scope of proposed CIP-012-1 is Real-time Assessment and Real-time monitoring data pertaining to more than just the field asset at which the transmitting Control Center is located.

2) Data in Scope

The SDT determined that Real-time Assessment and Real-time monitoring data exchanged between Control Centers should be subject to the protections of proposed CIP-012-1 due to the critical nature of the data. Reliability Coordinators and Transmission Operators must perform Real-time Assessments every 30 minutes to assess conditions on the system and determine whether there are any actual or potential exceedances of System Operating Limits or Interconnection Reliability Operating Limits.[14] In addition, Reliability Coordinators, Balancing Authorities, and Transmission Operators must perform Real-time monitoring.[15] Because entities operate and monitor the BES according to this Real-time information, it is of critical importance that it is accurate.

---

12 *Id*. at P 41 (citing the Notice of Proposed Rulemaking at P 59).

13 *Id*. at P 57.

14 Reliability Standards IRO-008-2, Requirement R4 and TOP-001-4, Requirement R13.

15 Reliability Standards IRO-002-5, Requirements R5 and R6 and TOP-001-4, Requirements R10 and R11.

Proposed CIP-012-1 excludes other data typically transferred between Control Centers, such as Operational Planning Analysis data, that is not used by the Reliability Coordinator, Balancing Authority, and Transmission Operator in Real-time. Although an Operational Planning Analysis provides information for the next-day operations, entities adjust their operating actions during the current day based on the data from Real-time Assessments and Real-time monitoring. If there is suspicion that Operational Planning Analysis data has been compromised, there is also time to verify the data prior to any impact on Real-time operations. The SDT thus determined that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in Reliability Standard CIP-002-5.1a.

More specifically, while Reliability Coordinators and Transmission Operators must perform an Operational Planning Analysis that includes an assessment of whether planned operations within their areas will exceed any System Operating Limits,[16] an entity will operate its system based on an assessment of the conditions on the day of operation as indicated by Real-time monitoring and Real-time Assessments. As a result, although an Operational Planning Analysis factors into how an entity operates, there is less of a risk that an entity would act on compromised data from an Operational Planning Analysis given it will base its operating actions on Real-time inputs. The SDT considered the role of an Operational Planning Analysis in BES operations and determined that there was a lower risk of affecting the reliability of the BES if Operational Planning Analysis data is compromised. Therefore, the SDT determined that this lower risk did not warrant the protections of proposed CIP-012-1. The SDT determined entities

[16] Reliability Standards IRO-008-2, Requirement R1 and TOP-002-4, Requirements R1.

should focus resources on Real-time inputs as those could adversely impact the reliable operation of the BES within 15 minutes.

While FERC also directed NERC to consider protecting data at rest, the SDT determined that because this data resides within BES Cyber Systems, the data is protected by CIP-003-6 through CIP-011-2. These protections include the following:

- ESPs: Data at rest stored on a high or medium impact BES Cyber System would reside within an ESP. The ESP provides a logical border around the network that can only be accessed through an Electronic Access Point. In addition, other protections are applied to the ESP that help ensure the data on the BES Cyber System is secure.

- Electronic access controls: Data at rest on low impact BES Cyber Systems within applicable Control Centers are protected by electronic access controls that permit only necessary inbound and outbound electronic access as required by Reliability Standard CIP-003-6.

- Physical security controls: In addition to ESPs and electronic access controls noted above, data at rest on low, medium, and high BES Cyber Systems are protected by physical controls, such as PSPs for some BES Cyber Systems, as required by Reliability Standards CIP-003-6 and CIP-006-6.

- Other protections: The CIP Reliability Standards also require other protections, such as training and cyber security awareness for personnel (CIP-003-6 and CIP-004-6); system security management (CIP-007-6); recovery plans for BES Cyber Systems (CIP-009-6); and BES Cyber System Information protection (CIP-011-2); among others, that promote the security of data at rest at Control Centers.

As a result of the protections included in the CIP Reliability Standards, the SDT only included protections for data while being transmitted between Control Centers in proposed CIP-012-1.

Similarly, oral communication is out of scope. The SDT concluded that oral communications do not need additional protections under proposed CIP-012-1 because operators have the ability to terminate the call and initiate a new one via trusted means if they suspect a problem with, or compromise of, the communication channel. In fact, Reliability Standard COM-001-3 requires Reliability Coordinators, Balancing Authorities, and Transmission Operators to have Alternative Interpersonal Communication capability with certain entities. As a result, these

entities would be able to use the Alternative Interpersonal Communication capability if an individual suspected a compromise of oral communications on one channel. Given this ability, proposed CIP-012-1 does not require protections for oral communications.

C. Requirements of Proposed Reliability Standard CIP-012-1

Proposed Reliability Standard CIP-012-1 consists of a single requirement that requires Responsible Entities to develop plans to meet the security objective of mitigating the risks posed by unauthorized modification and unauthorized disclosure of Real-time Assessment and Real-time monitoring data. Although proposed CIP-012-1 prescribes some items to include in the plan, it allows Responsible Entities to develop and implement a plan that works best for their operational environment while meeting the security objective. The use of a plan is consistent with other CIP Reliability Standards, and the objective allows the Reliability Standard to maintain relevancy while the technology used by Responsible Entities to meet the objective of CIP-012-1 continues to evolve and improve.

In proposed CIP-012-1, the SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Proposed Reliability Standard CIP-012-1 includes the following requirement and parts, each of which is discussed below:

> **R1.** The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]
>
> **1.1.** Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-

time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

Requirement R1 mandates that each Responsible Entity develop a plan to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. Responsible Entities must include the following in their plans: (1) identification of security protections (Part 1.1); (2) identification of where these protections are applied (Part 1.2); and (3) identification of the responsibilities of each party if the communicating Control Centers are owned or operated by different Responsible Entities (Part 1.3).

Specifically, pursuant to Part 1.1, Responsible Entities must include the identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers. Responsible Entities may choose logical protection, physical protection, or a combination of both as long as the protections meet the security objective of mitigating the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers. As a result, Responsible Entities have the latitude to determine which controls are appropriate for their organization, so long as those controls meet the security objective.

This approach is consistent with the principles for development as articulated by NERC in its comments to the FERC Notice of Proposed Rulemaking,[17] with which FERC agreed: protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to account for the range of technologies and entities involved in bulk electric system communications.[18]

Pursuant to Part 1.2, Responsible Entities must include in their plans the identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers. The identification of where security protection is applied (CIP-012-1 Requirement R1, Part 1.2) promotes alignment with the identification of Responsible Entity responsibilities (CIP-012-1 Requirement R1, Part 1.3) and helps with evaluating the overall effectiveness of the protections used.

Pursuant to Part 1.3, Responsible Entities must include in their plans the identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers if the Control Centers are owned or operated by different Responsible Entities. This requirement part does not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data, but it provides a clear expectation that Responsible Entities must sort out

---

[17] *Comments of the North American Electric Reliability Corporation in Response to Proposed Rulemaking*, at 20-21 Docket No. RM15-14-000 (Sept. 21, 2015).

[18] Order No. 822 at P 55.

responsibilities to help ensure that appropriate protections are in place. Where data is transmitted between different entities, the SDT determined that it is necessary for both entities to understand the responsibilities of applying security controls to ensure the data is protected through its entire transmission. This requirement part will help ensure there is no security gap.

As noted above, in Order No. 822, FERC stated that NERC should develop measures to protect the confidentiality, integrity, and availability of sensitive BES data. To that end, proposed CIP-012-1 requires entities to implement protections for the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of Real-time Assessment and Real-time monitoring data. The availability of such data is addressed in existing Reliability Standards. As FERC stated, "[p]rotecting the availability of [BES] data involves ensuring that required data is available when needed for [BES] operations." [19] Reliability Standard IRO-002-5 requires redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center in order to exchange Real-time data used in Real-time monitoring and Real-time Assessments with Balancing Authorities, Transmission Operators, and other entities the Reliability Coordinator deems necessary. Similarly, Reliability Standard TOP-001-4 requires Balancing Authorities and Transmission Operators to have redundant and diversely routed data exchange infrastructure to exchange Real-time data. The redundancy of data exchange infrastructure helps to ensure the availability of critical Real-time data for Control Centers. Additionally, Reliability Standards IRO-010-2 and TOP-003-3 require Reliability Coordinators, Transmission Operators, and Balancing Authorities to use a mutually agreeable security protocol for exchange of Real-time data. By agreeing on the same security protocol, entities communicate directly with the appropriate entities rather than having to translate different protocols, which

[19] Order No. 822 at P 54 n.60.

further helps to ensure the availability of Real-time data. As a result, the SDT determined that the confidentiality, integrity, and availability of Real-time Assessment and Real-time monitoring data would be protected by requirements in the suite of Reliability Standards, including proposed CIP-012-1.

D. Enforceability of Proposed Reliability Standard

The proposed Reliability Standard also includes a measure that supports the requirement by clearly identifying what is required and how the ERO will enforce the requirement. The measure helps 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 a VRF and VSLs. The VRF and VSLs provide guidance on the way that NERC will enforce the requirement of the proposed Reliability Standard. The VRF and VSLs for the proposed Reliability Standard comport with NERC and FERC guidelines related to their assignment. Exhibit G provides a detailed review of the VRF and VSLs, and the analysis of how the VRF and VSLs were determined using these guidelines.

V. EFFECTIVE DATE

NERC respectfully requests the proposed Reliability Standard 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, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) 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 CIP012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the date the standard is adopted

by the NERC Board, or as otherwise provided for in that jurisdiction.The 24-month implementation period is designed to afford Responsible Entities sufficient time to implement the new controls and coordinate with other Responsible Entities that own or operate Control Centers as required in proposed Reliability Standard CIP-012-1.

VI. CONCLUSION

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

- proposed Reliability Standard CIP-012-1, and associated elements included in Exhibit A, effective as proposed herein; and
- the proposed Implementation Plan included in Exhibit B.

Respectfully submitted,

/s/ Marisa Hecht

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: October 4, 2018

EXHIBITS A - B and D - I

EXHIBIT C

Reliability Standards Criteria

The discussion below explains how the proposed Reliability Standard meets or exceeds the 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 and expands the protections required by NERC's CIP Reliability Standards by requiring Responsible Entities to protect the confidentiality and integrity of certain Real-time sensitive data pertaining to Real-time operations while being transmitted between BES Control Centers, consistent with the FERC directive in Order No. 822[1]. Specifically, proposed Reliability Standard CIP-012-1 improves reliability by requiring Responsible Entities to develop a plan to mitigate the risks posed by unauthorized modification and unauthorized disclosure of Real-time Assessment and Real-time monitoring data. The plan must include the following three components: (1) identification of security protection used to meet the security objective; (2) identification of where the Responsible Entity applied the security protection; and (3) identification of the responsibilities of each Responsible Entity for applying the security protection, if the communicating Control Centers are owned by different entities. Exhibit F includes technical rationale for the proposed Reliability Standard to demonstrate the technical soundness of the means to achieve the reliability goal.

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

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, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners that own or operate a Control Center. 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 Factor 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 G. The assignment of the severity level for each VSL is consistent with the corresponding requirement. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability 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 requirement by clearly identifying what is required to demonstrate compliance. These measures help provide clarity regarding the manner in which the requirement will be enforced and help ensure that the requirement 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. 822 and requires protections for Control Centers containing BES Cyber Systems of any impact level.

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 for mitigating the risks posed by unauthorized disclosure and unauthorized

modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. 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 24-month 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, develop infrastructure, coordinate among other entities, or develop other relevant capability.

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 H includes a summary of the development proceedings and details the processes followed to develop the proposed Reliability Standard. These processes included, among other things, comment and ballot periods. Additionally, all meetings of the drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum, and the last two additional ballots and final ballot exceeded the required ballot pool approval levels.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.

NERC has identified no competing public interests regarding the request for approval of the proposed Reliability Standard. No comments were received that indicated the proposed Reliability Standard conflicts with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.

No other negative factors relevant to whether the proposed Reliability Standard is just and reasonable were identified.