UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Critical Infrastructure Protection Reliability	)	
Standard CIP-012-1 – Cyber Security –	)	Docket No. RM18-20-000
Communications between Control Centers	)	

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-012-1 (Cyber Security – Communications between Control Centers).[1] NERC supports the Commission's proposal to approve the proposed Reliability Standard. As discussed in the NOPR, proposed Reliability Standard CIP-012-1 improves upon the currently effective CIP Reliability Standards by: (1) mitigating cyber security risks associated with communications between Bulk Electric System ("BES") Control Centers; (2) supporting situational awareness; and (3) protecting the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between BES Control Centers.[2]

As provided in these comments, NERC does not support the Commission's NOPR proposal to direct modifications to the CIP Reliability Standards to: (1) require protections regarding the availability of communication links and data between BES Control Centers; and (2) provide additional specificity on the types of data that must be protected.[3] Instead of a directive to modify

[1] *Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers*, 167 FERC ¶ 61,055 (2019) ("NOPR").

[2] NOPR at P 2.

[3] NOPR at P 4.

the CIP Reliability Standards, NERC proposes to conduct a study of the risks to availability of data and communication links between Control Centers to determine an appropriate course of action.

I. COMMENTS

NERC does not support the proposed directives. First, Section I.A discusses how the currently effective Reliability Standards and proposed CIP-012-1 already include requirements that help address the risks associated with the unavailability of communication links and data between Control Centers. As it is unclear whether any additional protections are both needed and feasible, NERC proposes to initiate a study on this issue rather than modify the CIP Reliability Standards. Second, Section I.B discusses how the language in proposed CIP-012-1 is sufficient for entities to identify the data subject to the proposed standard.

A. Proposed Directive to Modify Standard to Address Availability

In the NOPR, the Commission proposes to direct NERC to modify the CIP Reliability Standards to include availability protections for data and communication links between Control Centers. Availability is one of three information security objectives that cyber security protections seek to support.[4] In Order No. 822, the Commission noted that, "Protecting the availability of [BES] data involves ensuring that required data is available when needed for [BES] operations."[5]

[4] The National Institute of Standards and Technology ("NIST") defines Security Objective as "Confidentiality, integrity, or availability." *Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations* app. B, at B-22 (2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf ("NIST 800-53").

[5] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037 at P 54 n.60 (2016) ("Order No. 822").

The National Institute of Standards and Technology ("NIST") describes the following methods, among others, to protect availability of data:[6]

- Redundant or alternate systems or infrastructure.[7]
- Recovery of information systems.[8]
- Emergency disabling of encryption.[9]

Other controls can also help support availability. For example, the use of the same communications protocol between different entities helps to ensure entities can communicate effectively. Similarly, alerts on disruption of service help inform entities of when to perform corrective actions to receive the information needed in a timely manner.

As discussed further below, NERC does not support the Commission's proposed directive at this time. Existing NERC Reliability Standards provide protections of data and communication links between Control Centers, including some that align with the recommendations from the NIST framework. Instead of a directive to revise the CIP Reliability Standards, NERC proposes to conduct a study of the currently enforceable protections within NERC Reliability Standards, assess whether any risks to availability remain, and, if any residual risks are found, evaluate cost effective alternatives for addressing these risks.

[6] These protection methods are highlighted in NIST 800-53 at 35 (citing to the control documents appended to the publication that provide additional detail on the controls) as ways to address availability.

[7] *See* NIST 800-53 app. F-CP at F-83 to F-87 (controls CP-6, CP-7, CP-8, and CP-9).

[8] *See* NIST 800-53 app. F-CP at F-87 to F-88 (control CP-10).

[9] *See* NIST 800-53 app. F-SC at F-195 to F-196 (control SC-12).

1. <u>Existing NERC Reliability Standards, along with proposed CIP-012-1, help to address the risks related to unavailability of data and communication links between Control Centers.</u>

As NERC explained in its petition for approval of proposed CIP-012-1, existing NERC Reliability Standards require entities to implement controls that help address the risks related to unavailability of data and communication links between Control Centers.[10] Several of NERC's existing Reliability Standards complement the CIP Reliability Standards and are designed to support availability, as that concept is understood in the information security sector, of data and communication links between Control Centers. These standards obligate entities to take steps to protect availability; the protection of availability is not merely an outcome. As a result, NERC would not duplicate these obligations in the CIP Reliability Standards in order to achieve NERC's reliability goals in an efficient and effective manner.

a. *NERC Reliability Standards support availability of data between Control Centers.*

Reliability Standards that require one or more availability protections are discussed below. Collectively, these protections help support the availability of data and communication links by: (1) requiring redundant data exchange infrastructure within Control Centers; (2) requiring a mutually agreeable security protocol for exchanging Real-time monitoring and Real-time Assessment data; (3) requiring entities to address data quality and to notify System Operators when Real-time monitoring alarm processors are not working properly; (4) requiring recovery plans for Control Center data exchange infrastructure that are medium and high impact BES Cyber Systems, or their associated Electronic Access Control or Monitoring Systems ("EACMS") or Physical Access Control Systems ("PACS"); (5) enabling entities to disable encryption during certain CIP

[10] *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-012-1* at 17-18, Docket No. RM18-20-000 (Sept. 18, 2018).

Exceptional Circumstances; and (6) requiring backup Control Center facilities or backup Control Center functionality.

i. IRO and TOP Reliability Standards

NERC developed the IRO and TOP Reliability Standards using availability of data as a guiding principle. In fact, one of the Reliability and Market Interface principles that the IRO and TOP Reliability Standards support is that "Information necessary for the planning and operation of interconnected bulk power systems *shall be made available* to those entities responsible for planning and operating the systems reliably."[11] (emphasis added) As a result, the requirements within the standards described below help to support availability.

As noted above, the NIST framework includes redundancy of infrastructure or systems as a control that supports availability. IRO-002-5 and TOP-001-4 require Reliability Coordinators ("RCs"), Balancing Authorities ("BAs"), and Transmission Operators ("TOPs") to have redundant and diversely routed data exchange infrastructure for Real-time Assessment and Real-time monitoring data within a Control Center.[12] As such, the requirements for diversely routed data exchange infrastructure for Real-time Assessment and Real-time monitoring data within Control Centers align with suggested protections of availability in the NIST framework.

While IRO-002-5 and TOP-001-4 cover infrastructure within Control Centers, not between Control Centers, the requirements help protect the availability of data to be exchanged between Control Centers. While located within the Control Center, the data exchange infrastructure in scope

[11] *Standards Authorization Request Form* for Modifications to TOP and IRO Standards at 4, available in *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards IRO-002-5 and TOP-001-4*, Exhibit F at 174, Docket No. RD17-4-000 (Mar. 6, 2017); *Standards Authorization Request Form* for Project 2014-03 Revisions to the TOP/IRO Reliability Standards at 6, available in *Petition of the North American Electric Reliability Corporation for Approval of Proposed Transmission Operations and Interconnection Reliability Operations and Coordination Reliability Standards*, Exhibit K at 483, Docket No. RM15-16-000 (Mar. 18, 2015).

[12] IRO-002-5, Requirement R2 and TOP-001-4, Requirement R20.

of these requirements facilitates sending and receiving data between Control Centers. If, for instance, an applicable entity lost capability of some of this data exchange infrastructure, the applicable entity could continue to send and receive data between Control Centers because of the redundant data exchange infrastructure within its Control Center. Thus, protections applied within a Control Center help support data exchange, as well as data availability, between Control Centers.

IRO-010-2 and TOP-003-3 require applicable entities to use a mutually agreeable security protocol between Control Centers.[13] This supports availability by helping to ensure that conflicting protocols do not impede receipt of data between Control Centers.

IRO-018-1(i) and TOP-010-1(i) require RCs, BAs, and TOPs to address data quality and to have an alarm process monitor that provides notification to System Operators when Real-time monitoring alarm processors are not working properly.[14] These protections serve to alert entities to potential issues with systems receiving the data so that entities can address them in a timely manner, as timeliness is an important component of availability.[15] These protections help to ensure information is available when needed.

ii. CIP Reliability Standards

As noted above, the NIST framework suggests recovery of information systems as a control to support availability. Reliability Standard CIP-009-6 requires Responsible Entities to have, implement, and maintain recovery plans for medium and high impact BES Cyber Systems and their associated EACMS and PACS at Control Centers. The recovery plans can include the systems and infrastructure facilitating data exchange between Control Centers. Recovery of these systems

[13] IRO-010-2, Requirement R3 and TOP-003-3, Requirement R5.

[14] IRO-018-1(i), Requirements R1 and R3; TOP-010-1(i), Requirements R1 and R4.

[15] *See* NIST 800-53 app. B at B-2 (defining Availability as "Ensuring timely and reliable access to and use of information.").

helps to ensure that data continues to be available. Thus, the recovery plans help to support availability for certain data exchange systems used by Control Centers.

Proposed CIP-012-1 includes a provision for CIP Exceptional Circumstances ("CEC") in Requirement R1, which allows Responsible Entities to disable encryption of data if necessary. For example, if the entity's encryption system is not working, the entity could review whether the situation qualifies as a CEC and, if so, disable the encryption controls to support availability of needed data. As discussed above, disabling encryption controls is one suggested control for supporting availability according to the NIST framework.

b. NERC Reliability Standards support availability of communication links.

Reliability Standard EOP-008-2 helps support the availability of communication links between Control Centers by requiring RCs to have backup Control Center facilities, or backup Control Center functionality for BAs and TOPs, in addition to their primary Control Centers. These backup facilities supply redundancy of some communication links and data exchange infrastructure and capabilities at the backup Control Center.[16] For entities with geographically diverse primary and backup Control Centers, some communication links are physically separate from one another. While geographic diversity alone will not always provide redundancy of communication links, having backup Control Centers with different paths to communicate with other Control Centers helps support availability of communication links.

c. NERC does not seek to duplicate obligations in the CIP Reliability Standards that exist in other Reliability Standards.

The protections described above directly support availability and must be implemented to comply with the standards. NERC does not support duplicating these same protections within the CIP standards. As stated in Order No. 693, "While a Reliability Standard does not necessarily need

[16] EOP-008-2, Requirement R3.

to reflect the optimal method for achieving its reliability goal, a Reliability Standard should achieve its reliability goal effectively and efficiently."[17] As such, NERC seeks to ensure that its suite of Reliability Standards are effective and efficient and do not duplicate protections. Duplicating protections is not needed for reliability and can create unnecessary administrative and compliance burdens on entities.

In fact, consistent with the objective for effective and efficient Reliability Standards, NERC is undertaking a Standards Efficiency Review initiative to help ensure that Reliability Standards support reliability in a clear and concise manner and do not duplicate requirements.[18] As part of this initiative, NERC is proposing retirement of redundant requirements whose required performance is inherent to the performance of other Reliability Standard requirements.[19] Obligating Responsible Entities to implement protections under the CIP Standards that are required under other standards would be contrary to the goal of efficiency and to initiatives designed to further that goal.

2. In lieu of a directive, NERC proposes to conduct a study to assess whether additional protections for availability of data and communication links between Control Centers are needed and feasible.

As noted in Section I.A.1 above, existing Reliability Standards require entities to implement controls that help mitigate the risks related to unavailability of data and communications links. NERC recognizes that there may be additional controls that could help address these risks. NERC understands, however, that many of these controls would involve communication links that are owned by a third-party telecommunications provider. There may be

[17] Order No. 693 at P 5.

[18] Information on the Standards Efficiency Review initiative is available at https://www.nerc.com/pa/Stand/Pages/Standards-Efficiency-Review.aspx.

[19] *See Petition of the North American Electric Reliability Corporation for Approval of Revised and Retired Reliability Standards Under the NERC Standards Efficiency Review*, Docket No. RM19-17-000 (June 7, 2019).

challenges for Responsible Entities to develop, implement, and enforce required controls for those third-party links. Moreover, depending on the magnitude and type of controls, some may be infeasible to implement. Assessing the feasibility of any additional protections is consistent with the Commission's charge for NERC to address the risk to availability with controls that can be "implemented in a reasonable manner."[20] As a result, a data-driven approach to considering the risks, such as a study, will help to address this issue in the most efficient and effective manner.

Based on these considerations, NERC does not support a directive to modify the Reliability Standards to address availability at this time. Instead, NERC proposes that the Commission accept a commitment from NERC to study the risks to availability of data and communication links between Control Centers and the current controls that support availability. Specifically, NERC plans to consider the following in its study: (1) how Control Centers communicate with one another; (2) ownership of communication links; (3) how Responsible Entities work with vendors to support availability of communication links; (4) controls used to support resiliency and availability of data and communication links; and (5) feasibility of Responsible Entities' implementing controls when communication links are owned by organizations not subject to NERC Reliability Standards. This study will help NERC determine the reasonableness of developing mandatory standards to require additional controls, if warranted, or take another appropriate and feasible course of action based on the resulting analysis. NERC should have the opportunity to appropriately scope the study, conduct the study, and develop a fuller record prior to engaging in any standards development activity, if necessary. If the Commission accepts NERC's commitment, NERC would submit a report to FERC within 18 months of the effective date of CIP-012-1.

[20] NOPR at P 20.

B. Proposed Directive to Modify Standard to Further Identify the Data in Scope

In the NOPR, the Commission noted that Real-time monitoring is not a NERC Glossary definition.[21] The Commission also asserted that proposed CIP-012-1 does not specify the types of data to be protected. As a result, the Commission proposed a directive to identify the types of data to be protected. The Commission also sought comments on whether NERC should define Real-time monitoring data. As explained below, further identification of the data, such as through the development of a NERC Glossary definition of Real-time monitoring, is not needed in proposed CIP-012-1.

The language used in proposed Reliability Standard CIP-012-1, "Real-time Assessment and Real-time monitoring data," is sufficient to identify the data as described in TOP-003-3 and IRO-010-2. Aside from proposed CIP-012-1, the IRO and TOP families are the only currently enforceable Reliability Standards that use the phrase "Real-time monitoring" and the term "Real-time Assessments." Reliability Standards TOP-003-3 and IRO-010-2 require entities to maintain data specifications, including minimum criteria, for the data necessary to perform Real-time monitoring and Real-time Assessments.[22] Compliance with these standards defines the data that is used in Real-time monitoring and Real-time Assessments. By using this language that is only referenced in the IRO and TOP Reliability Standards families, proposed CIP-012-1 brings the data identified pursuant to TOP-003-3 and IRO-010-2 into scope. As such, NERC does not support further identification of the data protected under proposed CIP-012-1.

[21] NOPR at P 3. The Glossary of Terms Used in NERC Reliability Standards ("NERC Glossary") is at https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[22] IRO-010-2, Requirement R1 and TOP-003-3, Requirements R1 and R2.

While a cross-reference to the standards where the data is defined may help to reiterate the scope of data, NERC does not believe it is necessary given the sufficiency of the language used in proposed CIP-012-1 and the administrative upkeep of adding a cross-reference.

Furthermore, a NERC Glossary definition for "Real-time monitoring" in proposed CIP-012-1 could have the unintended consequence of narrowing the scope of data subject to the standard. A definition of "Real-time monitoring" specific to CIP-012-1 may not capture all the data used to perform Real-time Assessments and Real-time monitoring as identified in a data specification under TOP-003-3 or IRO-010-2 if an entity identified data not included in the definition. This may inadvertently lead to some of this data not being protected under CIP-012-1. However, under the currently proposed CIP-012-1, this data would be in scope and subject to CIP-012-1 protections.

II. CONCLUSION

NERC respectfully requests that the Commission consider these comments and approve proposed Reliability Standard CIP-012-1.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: June 24, 2019