UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE ISO/RTO COUNCIL

The ISO/RTO Council ("IRC")[1] respectfully submits these comments in response to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR"), which proposes to approve Critical Infrastructure Protection Reliability Standard CIP-012-1 (Cyber Security – Communications between Control Centers) and to direct that the North American Electric Reliability Corporation ("NERC") develop certain modifications to Reliability Standard CIP-012-1.[2]

The IRC generally supports the Commission's proposed approval of Reliability Standard CIP-012-1 as submitted by NERC to the Commission on September 18, 2018. The IRC provides these comments in order to request that the Commission reconsider, and in the alternative clarify, its proposed directives that NERC further modify the Critical Infrastructure Protection ("CIP") Reliability Standards in order to: (1) require

[1] The IRC comprises the Alberta Electric System Operator ("AESO"), the California Independent System Operator Corporation ("CAISO"), the Electric Reliability Council of Texas, Inc. ("ERCOT"), the Independent Electricity System Operator ("IESO"), ISO New England Inc. ("ISO-NE"), the Midcontinent Independent System Operator, Inc. ("MISO"), the New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection, L.L.C. ("PJM"), and the Southwest Power Pool, Inc. ("SPP"). AESO is not subject to the Commission's jurisdiction. Therefore, AESO is not joining these comments. Individual IRC members may also file separate comments.

[2] *Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers*, NOPR, 84 Fed. Reg. 17105 (April 24, 2019), 167 FERC ¶ 61,055 (2019).

protections regarding the availability of communication links and data communicated between bulk electric system Control Centers; and (2) more clearly identify the types of data that must be protected.

I. COMMENTS

A. Availability of Communication Links and Data Communicated between Control Centers

In the NOPR, the Commission proposes to direct that NERC develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers.[3] As NERC explains in its comments on the NOPR, a number of Reliability Standards already provide ample assurance of the availability of communications between Control Centers. The IRC agrees with NERC that additional requirements to support availability of communications are therefore unnecessary.

Moreover, any mandate to ensure continued availability of communications would be problematic because the physical data links between Control Centers are owned by third-party telecommunications service providers and not by the responsible entities subject to CIP-012. As such, requiring responsible entities to ensure the continuing availability of data links would impose a compliance obligation to maintain a service over which they have no direct control. In the IRC's view, only the owners of telecommunication facilities can assume responsibility for the availability of their systems. And although FERC may lack jurisdiction over telecommunication service providers, this fact cannot justify shifting legal liability for availability to entities that

[3] NOPR at P 27.

merely contract for services provided over telecommunications facilities.

The IRC acknowledges that FERC could require additional actions by responsible entities to *promote* the availability of these communications links to the extent possible through contracts with telecommunications providers. For example, NERC could adopt a standard that would require responsible entities, when negotiating these service contracts, to take reasonable steps or use best efforts to maximize the availability of communications links. Reasonable additional steps might include tailoring service level agreement terms to promote availability, using commercially reasonable efforts to secure redundant and diversely routed communication paths where available and verifiable,[4] and/or contracting with multiple service providers where available.

This type of "best efforts" approach would be consistent with the approach taken by NERC, and later approved by FERC, in connection with CIP Reliability Standard-013-1, which addressed supply chain security risks.[5] In that project, NERC proposed, and industry ultimately approved, language recognizing that responsible entities cannot force software and hardware vendors to agree to terms related to disclosure of responses to cybersecurity breaches.[6] Consequently, the standard required development of a risk management plan that includes a "process" to "address" such measures in the procurement process.[7] Similarly, responsible entities' inability to require

---

[4] Verification of the redundancy or diverse routing of telecommunications paths is not always verifiable because telecommunications service providers frequently regard this information as confidential.

[5] *See* NERC Reliability Standard CIP-013-1, Requirement R2; *Supply Chain Risk Management Reliability Standards*, Final Rule, 83 Fed. Reg. 53,992 (Oct. 26, 2018) (Order 850).

[6] *Id.*, excluding "the actual terms and conditions of a procurement contract" from the scope of the requirement.

[7] *Id.*

telecommunications providers to guarantee availability of their networks suggests that a similar approach may be appropriate with respect to CIP-012. Such an approach could increase availability protections but also alleviate the concern that responsible entities cannot be required to ensure availability of facilities they do not own or control.

Finally, if the Commission believes a workshop would be helpful to allow further discussion of how best to address the availability of communications networks, the IRC would be amenable to participating. The IRC sees potential value in exploring ways to maximize availability without imposing an unworkable mandate.

B. Identification of Data

The Commission also proposes to direct NERC to develop modifications to the CIP Reliability Standards to clearly identify the types of data that must be protected.[8] As proposed, CIP-012-1 specifies that the requirements in R1 apply to data used in Real-time Assessments and Real-time monitoring. The NOPR observes that while the term "Real-time Assessment" is defined in the NERC Glossary of Terms, "Real-time monitoring" is not defined there, nor are the types of data used for either Real-time Assessments or Real-time monitoring specified in the standard. The NOPR expresses the concern that this could lead to inconsistent implementation and enforcement.[9]

The IRC submits that the scope of data subject to protection under CIP-012-1 is sufficiently clear, as all responsible entities must already know the universe of data needed for Real-time Assessment and Real-time monitoring activities in order to comply with NERC Reliability Standards TOP-003-3 and IRO-010-2. These standards require

[8] NOPR at P 34.

[9] *Id*. at 30.

Transmission Operators and Reliability Coordinators to "maintain a documented specification for the data necessary for . . . Operational Planning Analyses, Real-time monitoring, and Real-time Assessments," and require other responsible entities, including Generator Operators and Transmission Operators, to provide data to the Transmission Operator and Reliability Coordinator consistent with that specification.[10] Though "Real-time monitoring" is not defined, the IRC sees no reason that the term should be presumed to mean something different from what it means in other places where it is used in the NERC Reliability Standards.

However, the IRC would not oppose further clarification in CIP-012-1—consistent with the Technical Rationale that accompanies the proposed standard—to provide that the data required to be protected is the same data required for Real-time Assessments and Real-time monitoring activities *undertaken pursuant to TOP-003 and IRO-010*.[11] The inclusion of an express reference to TOP-003-3 and IRO-10-2 in CIP-012 would be more than sufficient to clarify what information must be protected.

The IRC would not support revising CIP-012-1 to identify each specific type of data used in Real-time Monitoring or Real-time assessments, as this would be unworkable. The specific types of data needed for these activities varies from entity to

[10] NERC Reliability Standard TOP-003-3, Requirements R1, R3; IRO-110-2, Requirements R1, R3.

[11] To the extent cross-referencing presents a practical concern that a change to the version of one standard may require an update to other standards that cite to that standard, this problem can be alleviated by avoiding references to specific standard versions or by allowing the drafting team, the Standards Committee, or NERC to make these purely administrative changes as part of the standard development process.

entity and sometimes include several hundred discrete items.[12] In fact, it is for this same reason that TOP-003-3 and IRO-010-2 do not specify what specific types of data are required for those critical RC and TOP activities. And if TOP-003-3 and IRO-010-2 are not required to be more specific, it is unclear why a standard governing protection of communications made pursuant to those standards should be.

Additionally, the IRC submits that defining "Real-time monitoring" in the NERC Glossary of Terms would not be particularly helpful, as this would provide no greater clarity than exists today under TOP-003-3 and IRO-010-2 concerning the types of data required for that activity. The data specifications maintained by Reliability Coordinators and Transmission Operators under those standards already adequately describe what data is included in Real-time Assessment and Real-time monitoring.

To the extent the Commission believes additional clarification is needed, the IRC requests that the Commission clarify that an express reference to TOP-003 and IRO-010 in CIP-012-1 is sufficient to identify the data that must be protected.

II. CONCLUSION

The IRC respectfully requests the Commission give due consideration to the foregoing comments before issuing a final rule.

[12] *See* e.g. ERCOT NERC IRO 010 and TOP 003 Mapping Document V4, *available at* http://www.ercot.com/content/wcm/key_documents_lists/89338/NERC_IRO-010_and_TOP-003_Mapping_Document_V4.xlsx (identifying types of data used by ERCOT for Operations Planning Assessment, Real-time Assessment, and Real-time monitoring).

Respectfully submitted,

/s/ Roger E. Collanton
Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ Robert E. Fernandez
Robert E. Fernandez, General Counsel
Raymond Stalter,
Director of Regulatory Affairs
Carl Patka, Assistant General Counsel
Christopher R. Sharp, Senior Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
csharp@nyiso.com

/s/ Maria Gulluni
Maria Gulluni
Vice President and General Counsel
Margoth R. Caley
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

/s/ Craig Glazer
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
PJM Interconnection, L.L.C.
Suite 600
1200 G Street, N.W.
Washington, D.C. 20005
202-423-4743
craig.glazer@pjm.com
james.burlew@pjm.com

/s/ Andre T. Porter
Andre T. Porter
Vice President, General Counsel & Secretary
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
aporter@misoenergy.org

/s/ Chad V. Seely
Chad V. Seely
Vice President and General Counsel
Nathan Bigbee
Assistant General Counsel
Brandon Gleason
Senior Corporate Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
nathan.bigbee@ercot.com

/s/ Devon Hube
Devon Huber
Sr. Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto Ontario M5H1T1
Canada

/s/ Paul Suskie
Paul Suskie
Executive Vice President, Regulatory Policy & General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

Dated: June 24, 2019

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Austin, Texas this 24th day of June, 2019.

/s/ Nathan Bigbee
Nathan Bigbee
Assistant General Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744