UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Systems in Control Centers	Docket No. RM16-18-000

COMMENTS OF THE AMERICAN PUBLIC POWER ASSOCIATION, LARGE PUBLIC POWER COUNCIL, AND TRANSMISSION ACCESS POLICY STUDY GROUP

On July 21, 2016, the Commission issued a Notice of Inquiry seeking comment on possible modifications to the Critical Infrastructure Protection ("CIP") reliability standards regarding the cybersecurity of Control Centers.[1] The American Public Power Association ("APPA"), the Large Public Power Council ("LPPC"), and the Transmission Access Policy Study Group ("TAPS") (collectively, the "Joint Commenters") appreciate the opportunity to comment on this NOI.

INTEREST OF JOINT COMMENTERS

APPA is the national service organization representing the interests of not-for-profit, publicly owned electric utilities throughout the United States. More than 2,000 public power systems provide over 14% of all kilowatt-hour sales to ultimate customers and serve over 48 million people, doing business in every state except Hawaii. Public power systems own approximately 10.3% of the total installed generating capacity in the United States. Approximately 264 APPA members are subject to compliance with North American Electric Reliability Corporation ("NERC") standards applicable to users, owners, and operators of the Bulk Power System.

---

[1] *Cyber Systems in Control Centers*, 81 Fed. Reg. 49,641 (July 28, 2016), 156 FERC ¶ 61,051 (2016) ("NOI").

LPPC is an association of the 25 largest state-owned and municipal utilities in the nation. LPPC members are located throughout the nation, both within and outside RTO boundaries. LPPC represents the larger, asset owning members of the public power sector.

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states, promoting open and non-discriminatory transmission access.[2] TAPS members have long recognized the importance of grid reliability. As TDUs, TAPS members are users of the Bulk Power System, highly reliant on the reliability of facilities owned and operated by others for the transmission service required to meet TAPS members' loads. In addition, many TAPS members participate in the development of and are subject to compliance with NERC reliability standards.

[2] David Geschwind, Southern Minnesota Municipal Power Agency, chairs the TAPS Board. Jane Cirrincione, Northern California Power Agency, is TAPS Vice Chair. John Twitty is TAPS Executive Director.

Communications regarding these proceedings should be directed to:

Allen Mosher
Vice President, Policy Analysis
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
Tel.: (202) 467-2900
E-mail: amosher@publicpower.org

For APPA
Randolph Elliott
Senior Regulatory Counsel
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
Tel.: (202) 467-2952
E-mail: relliott@publicpower.org

John Twitty, Executive Director
TRANSMISSION ACCESS POLICY STUDY GROUP
P.O. Box 14364
Springfield, MO 65814
Tel.: (417) 838-8576
E-mail: 835consulting@gmail.com

For TAPS
Cynthia S. Bogorad
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
Tel.: (202) 879-4000
Fax: (202) 393-2866
E-mail: cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

For LPPC
Jonathan D. Schneider
STINSON LEONARD STREET LLP
1775 Pennsylvania Avenue, NW, Suite 800
Washington, DC 20006
Tel.: (202) 728-3034
E-mail:
jonathan.schneider@stinsonleonard.com

COMMENTS

In response to lessons learned from the 2015 Ukraine cyberattack, the NOI seeks comments on two possible modifications to the CIP standards to address the cybersecurity of Control Centers: (1) to require separation between the Internet and Bulk Electric System ("BES") Cyber Systems in Control Centers performing transmission operator functions, and (2) to require application whitelisting for BES Cyber Systems in Control Centers.

Joint Commenters take to heart the need to assess carefully the recommendations made by the Department of Homeland Security in its February 25, 2016 Alert.[3] The Commission is right to seek input on the recommendations, and Joint Commenters look forward to that dialogue. However, as the NOI recognizes, the current CIP standards already protect against unauthorized interactive remote access, unauthorized physical access, and malware.[4] Moreover, NERC is in the process of developing further revisions to the CIP standards that are related to the changes proposed in the NOI.[5] The Commission should allow NERC adequate time to evaluate the effectiveness of the existing CIP standards, which just became effective for High and Medium Impact systems on July 1, 2016,[6] before considering further modifications. Additional time will allow for a better understanding of the need for controls like those discussed in the NOI and the potential implications of such controls on operations. Joint Commenters therefore support NERC's request that the Commission not direct modifications to the CIP standards at this time.[7]

As discussed in NERC's comments, while requiring separation between the Internet and BES Cyber Systems in Control Centers performing transmission operator

---

[3] *See* Department of Homeland Security, Alert (IR-ALERT-H-16-056-01), *Cyber-Attack Against Ukrainian Critical Infrastructure* (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[4] NOI, P 1 & n.4.

[5] *See* NERC, Standards Authorization Request Form for Project 2016-02 – Modifications to CIP Standards (June 1, 2016), http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/CIP_SAR_822_directives_V5TAG_2016June1_clean.pdf. The scope of the changes include modification to the definition of "Low Impact External Routable Connectivity," and the impact designation for BES Cyber Systems associated with control centers performing the functional obligations of a transmission operator. *Id.*

[6] CIP requirements applicable to Low Impact systems must be implemented by April 1, 2017.

[7] *See* NERC's comments filed today in this docket.

functions and requiring application whitelisting for BES Cyber Systems in Control Centers may help reduce cybersecurity threats and vulnerabilities, mandating such prescriptive controls may also unduly limit operational flexibility without proportionate reliability benefits. The Commission should afford NERC and the industry the time to further evaluate the impact of those protections on operations to understand when and how those protections could be implemented without undue interference with the operational needs of Responsible Entities.

Moreover, we fully agree with NERC that additional directives at this time would increase an already significant workload for NERC and industry with respect to implementation of, and development of modifications to, the CIP standards. The industry's resources are currently devoted to implementation of the CIP standards, both those requirements applicable to High and Medium Impact BES Cyber Systems, which only went into effect on July 1, 2016, and those requirements applicable to Low Impact BES Cyber Systems, whose implementation is not required until April 1, 2017. Additionally, NERC and industry resources are currently devoted to addressing Commission directives from Order Nos. 822[8] and 829,[9] as well as modifications to the CIP standards to address issues identified during implementation. Indeed, smaller entities that are subject to compliance with CIP standards beginning in April 2017 are already facing difficult choices on how to deploy their limited cybersecurity resources.

---

[8] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 81 Fed. Reg. 4177 (Jan. 26, 2016), 154 FERC ¶ 61,037 (2016) ("Order No. 822"), *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

[9] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 81 Fed. Reg. 49,878 (July 29, 2016), 156 FERC ¶ 61,050 (2016).

If the Commission proceeds with a rulemaking to implement either or both of these proposals, Joint Commenters urge the Commission to consider the following two recommendations.

First, any proposal should adhere to the risk-based framework that was the hallmark of the CIP Version 5 standards. Specifically, the Commission should clarify that the proposed changes would apply only to Control Centers designated as Medium or High Impact in accordance with CIP-002-5. The NOI's proposed modification to separate Control Centers from the Internet already reflects that risk-based approach, as it would apply only to Control Centers performing transmission operator functions.[10] The NOI's proposal to require application whitelisting at Control Centers should similarly adopt a risk-based approach.

Limiting new CIP standards to Medium and High Impact Control Centers would be consistent with the Commission's recent orders. In Order No. 791, the Commission declined to direct modifications to the CIP standards that would make *all* Control Centers Medium or High Impact,[11] accepting NERC's judgement that some small balancing area or generator Control Centers have only a low impact on BES reliability. Earlier this year, the Commission approved changes to the CIP standards that will require owners and operators of Low Impact Control Centers to take appropriate actions, commensurate with the lower risk of those assets, by implementing cybersecurity plans that meet specific

---

[10] All Control Centers used to perform the functional obligations of a Transmission Operator are designated as either High or Medium Impact. NERC CIP-002-5 – Cyber Security – BES Cyber Asset and BES Cyber System Categorization, Attachment I, §§ 1.3, 2.12.

[11] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,756, 72,766 (Dec. 3, 2013), 145 FERC ¶ 61,160, P 89 (2013), *corrected*, 78 Fed. Reg. 76,986 (Dec. 20, 2013), *on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

security objectives, including objectives related to electronic access.[12] Directing NERC to develop new, prescriptive standards that would apply to Low Impact Control Centers would be inconsistent with the risk-based approach the Commission rightly adopted in these orders.

Second, if the Commission directs changes to the CIP standards, it should respect the technical limitations of existing BES Cyber Systems at Control Centers. Mandatory application whitelisting, where it is technically feasible, may be a practical and effective way to mitigate against cyberattacks. But some Control Centers' BES Cyber Systems may not have the ability to implement application whitelisting, so other technical solutions may be more appropriate. Before considering such a directive, further information is needed to evaluate the extent to which application whitelisting is compatible with existing BES Cyber Systems at Control Centers.

Similarly, further study is needed on the technical limitations of implementing encryption or data diodes for communication to or between Control Centers.[13] Such technical solutions may require changes on multiple cybersystems owned by different entities, not all of which are easily compatible. This adds to the technical and operational difficulty of implementation, which must be better understood before imposing prescriptive requirements.

---

[12] Order No. 822.

[13] *See* NOI, P 11 (asking whether the use of data diodes would be reliable and appropriate).

CONCLUSION

The Commission should consider these comments as it evaluates the need to take action regarding cybersecurity of Control Centers.

Respectfully submitted,

/s/ Cynthia S. Bogorad

Jonathan D. Schneider
Jonathan P. Trotta
STINSON LEONARD STREET LLP
1775 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20006
(202) 728-3034

Attorneys for the
Large Public Power Council

Cynthia S. Bogorad
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 879-4000

Attorneys for the
Transmission Access Policy Study Group

Randolph Elliott
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive
Suite 1000
Arlington, VA 22202
(202) 467-2952

Attorney for the
American Public Power Association

September 26, 2016