UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Security Incident Reporting Reliability Standards	Docket Nos.	RM18-2-000 AD17-9-000

COMMENTS OF THE AMERICAN PUBLIC POWER ASSOCIATION, ELECTRICITY CONSUMERS RESOURCE COUNCIL, AND TRANSMISSION ACCESS POLICY STUDY GROUP

The American Public Power Association ("APPA"), the Electricity Consumers Resource Council ("ELCON"), and the Transmission Access Policy Study Group ("TAPS") submit these comments on the Commission's December 21, 2017 Notice of Proposed Rulemaking.[1] The Commission's NOPR proposes to direct the North American Electric Reliability Corporation ("NERC") to develop a modification to its reliability standards to increase the scope of mandatory reporting requirements for cyber security incidents.

Instead of issuing the proposed directive, the Commission should consider whether tools other than a new or revised reliability standard could better achieve the goal of improving awareness of existing and future cyber security threats and potential vulnerabilities. Alternatively, if the Commission nevertheless directs the development of a new or revised standard, the Commission should give NERC flexibility to define appropriate reporting thresholds for actual and attempted cyber security incidents. Additionally (and regardless of whether the Commission directs NERC to develop a standard or instead adopts an alternative approach), the Commission should explicitly

[1] *Cyber Security Incident Reporting Reliability Standards*, 82 Fed. Reg. 61,499 (proposed Dec. 28, 2017), 161 FERC ¶ 61,291 (2017) ("NOPR").

state that it is not directing changes to the existing reporting requirements for low impact systems, and that NERC should implement any directive in a way that does not change the obligations for low impact systems.

I. INTERESTS OF APPA, ELCON, AND TAPS

APPA is the national service organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities account for 15% of all sales of electric energy (kilowatt-hours) to ultimate customers and collectively serve over 49 million people in every state except Hawaii. Approximately 261 public power utilities are registered entities subject to compliance with NERC mandatory reliability standards.

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products from virtually every segment of the manufacturing community. ELCON members operate hundreds of major facilities and are consumers of electricity in the footprints of all organized markets and other regions throughout the United States. Many ELCON members also operate behind-the-meter generation and are NERC registered entities, and ELCON has actively participated in NERC's stakeholder and standards development processes. Reliable electricity supply is essential to its members' operations.

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

---

[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.

users of the Bulk Power System and are 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.

Communications regarding these proceedings should be directed to:

For APPA
John E. McCaffrey, Regulatory Counsel
Jack Cashin, Director of Policy Analysis & Reliability Standards
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
Email: jmccaffrey@publicpower.org
jcashin@publicpower.org

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

For ELCON
John P. Hughes
President & CEO
ELECTRICITY CONSUMERS RESOURCE COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
(202) 682-1390
Email: jhughes@elcon.org

John Twitty
Executive Director
TRANSMISSION ACCESS POLICY STUDY GROUP
PO Box 14364
Springfield, MO 65814
(417) 838-8576
Email: jtwitty@tapsgroup.org

II. COMMENTS

A. Modifying mandatory standards is not necessarily the best tool to achieve the goal of improving awareness of cyber security threats and potential vulnerabilities.

The NOPR explains that its proposed directive is intended "to improve awareness of existing and future cyber security threats and potential vulnerabilities."[3] That is an appropriate objective, but directing new or revised mandatory reliability standards is not

[3] NOPR, P 24.

the only tool that NERC and the Commission have for achieving that reliability objective. Mandatory standards, by their nature, cannot easily adapt to dynamic problems like cyber security threats. NERC's comments filed today in this proceeding recognize that alternate approaches, other than mandatory standards, should be used to achieve the goals the Commission seeks to achieve through the proposed directive.[4] Edison Electric Institute's comments, also filed today, describe several partnerships that are in place between registered entities and the federal government that help identify and improve awareness about cyber security threats and vulnerabilities. Importantly, these partnerships provide security tools that go beyond the potential mitigation of reliability standards.

Thus, particularly in the constantly evolving area of cyber security, which operates against the backdrop of rapidly changing technology, the Commission should consider and utilize the most flexible tools to achieve its reliability goals without imposing undue burden on registered entities.

B. If the Commission nevertheless issues a directive for a new or modified reliability standard, it should give NERC flexibility to define appropriate reporting thresholds for actual and attempted cyber security incidents.

The NOPR proposes to direct NERC to develop a revised reliability standard that would "include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP [Electronic Security Perimeter] or associated EACMS [Electronic Access Control and Monitoring System]."[5] If a Final Rule in this proceeding includes a directive to develop a new or revised standard, the

---

[4] NERC points to its existing authority under Section 1600 of its Rules of Procedure to collect data about cyber security incidents and vulnerabilities as preferable to a reliability standard.

[5] NOPR, P 30.

Commission should explicitly give NERC the flexibility to define appropriate reporting thresholds for attempted cyber security incidents.

As proposed, the NOPR's directive is potentially overbroad and could result in unduly burdensome reporting requirements that *reduce* awareness of significant cyber threats. Utilities experience near constant attempts to probe their firewalls to detect vulnerabilities. Requiring registered entities to report every attempted probe, even if the attempt is not a credible threat, could result in most utilities submitting multiple reports every day. Such a reporting obligation would be unduly burdensome on registered entities. Moreover, excessive reporting of non-credible attempts to compromise an EACMS would overwhelm the reports of credible attempts, thus making it more difficult to identify real cyber security threats and potential vulnerabilities.

The Commission should avoid such a result. If the Commission decides to direct a new or revised reliability standard, it should not include the proposed generic threshold of reporting *any* incidents that compromise or attempt to compromise an ESP or EACMS. Instead, it should give NERC sufficient flexibility to define appropriate reporting thresholds for attempted compromises of an ESP or EACMS so that the resulting standard is better able to advance its purpose of improving awareness of cyber security threats and potential vulnerabilities.

C. In any event, the Commission should clarify that it is not directing changes to the existing reporting requirements for low impact systems.

The NOPR appropriately focuses on medium and high impact BES cyber systems. The NOPR begins its discussion of the cyber security incident reporting threshold by discussing the existing reporting requirement in CIP-008-5, a standard that applies only

to medium and high impact systems. And the NOPR's proposed directive—to require reporting of incidents that compromise or attempt to compromise an ESP or EACMS—necessarily refer only to medium and high impact systems, because ESPs and EACMS are terms that do not apply to low impact systems.[6] Commission Staff confirmed at the December 21, 2017 Open Meeting that the NOPR's focus on ESPs and EACMS "limits the proposal to high- and medium-impact BES Cyber Systems," and that the NOPR is "not touching on 'low' at this point."[7]

The NOPR's exclusion of low impact systems from the proposed expanded reporting requirements is appropriate. CIP-003-6 already requires owners and operators of low impact systems to identify Reportable Cyber Security Incidents and notify the ES-ISAC of them.[8] Consistent with the risk-based approach of the CIP standards, the reporting obligations for low impact systems allows for more flexibility than the reporting obligations for medium and high impact systems.[9] The Commission approved the existing incident reporting requirements in CIP-003-6 as providing appropriate security controls for low impact systems.[10] Expanding the reporting obligation for low impact systems would be unduly burdensome and not commensurate with the lesser risk that those systems pose to BES reliability. Additionally, given that there are many more

---

[6] *See* Revised Critical Infrastructure Protection Reliability Standards, Order No. 822, 81 Fed. Reg. 4177 (Jan. 26, 2016), 154 FERC ¶ 61,037, P 75 (2016) ("Order No. 822") *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016) ("We decline to adopt the recommendations . . . to modify the standards to utilize the concept of Electronic Security Perimeters for low impact systems.").

[7] Transcript of Commission Open Meeting at 26:14-17 (Dec. 21, 2017), https://www.ferc.gov/CalendarFiles/20180104102157-transcript.pdf.

[8] NERC, Reliability Standard CIP-003-6, Attachment 1, Section 4.2.

[9] Specifically, CIP-003-6 does not have the one-hour time limit for initial notifications of Reportable Cyber Security Incidents that is in CIP-008-5.

[10] Order No. 822, P 2.

low impact systems than medium and high impact systems, expanding the reporting obligation for low impact system increases the risk of creating excessive reporting full of "noise" that would make it harder to identify real threats. Thus, by excluding low impact systems, the NOPR correctly focuses on the most significant security threats associated with ensuring reliability.

If the Commission proceeds to issue a directive in this proceeding—whether it be a directive to develop a standard or a directive to use another tool to achieve the same goal—it should make plain that the directive is not intended to include low impact systems. While the NOPR indicates that it excludes low impact systems, the Final Rule should say so explicitly. Doing so would avoid potential confusion that could arise in implementing the directive.[11] Thus the Commission should clarify, if it does issue a directive, that it is not directing changes to the existing reporting requirements for low impact systems, and that NERC should implement the directive in a way that does not change the obligations for low impact systems.

CONCLUSION

For the reasons discussed above:

- The Commission should consider approaches other than directing a new or modified reliability standard to achieve the objective of improving awareness of cyber security threats and vulnerabilities;

[11] For example, the defined terms Cyber Security Incident and Reportable Cyber Security Incident are used in both CIP-003-6 for low impact systems and CIP-008-5 for medium and high impact systems.

- Alternatively, if a directive is issued, the Commission should give NERC flexibility to define appropriate reporting thresholds for attempted cyber security incidents; and
- In any case, the Commission should explicitly clarify in the Final Rule that it is not directing changes to the existing reporting requirements for low impact systems.

Respectfully submitted,

/s/ Cynthia S. Bogorad

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

Transmission Access Policy Study Group

John E. McCaffrey, Regulatory Counsel
Jack Cashin, Director of Policy Analysis & Reliability Standards
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900

American Public Power Association

John P. Hughes, President & CEO
ELECTRICITY CONSUMERS RESOURCE COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
(202) 682-1390

Electricity Consumers Resource Council

February 26, 2018