UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE LARGE PUBLIC POWER COUNCIL

I. INTRODUCTION AND EXECUTIVE SUMMARY

These comments are filed by the Large Public Power Council ("LPPC") in response to the Federal Energy Regulatory Commission's ("FERC" or the "Commission") Notice of Proposed Rulemaking, issued in this docket on December 21, 2017.[1] LPPC appreciates FERC's interest in developing additional information regarding attempts to compromise Electronic Security Perimeters ("ESPs") and associated Electronic Access Control or Monitoring Systems ("EACMS"), but believes that the proposed directive may yield a substantial quantity of unhelpful information and confusing analyses, while needlessly burdening Registered Entities. For that reason, if FERC proceeds with a directive, LPPC recommends that the Commission take these measures:

- Before finalizing any directive, FERC should direct the North American Electric Reliability Corporation ("NERC") and industry to work together to establish a sensible threshold for determining which attempts to compromise ESPs and EACMS warrant reporting.
- The process of determining what information may productively be the focus of data collection might begin with a FERC-sponsored technical conference aimed at

[1] *Coordination of Protection Systems for Performance During Faults and Specific Training for Personnel Reliability Standard*, 161 FERC ¶ 61,159 (2017) ("NOPR").

defining the definitional threshold for any new reporting requirement and the range of assets to which it applies.

- FERC should provide NERC with the flexibility to employ a data request issued under Section 1600 of its Rules of Procedure ("ROP"), rather than a mandatory Reliability Standard.

A. LPPC

LPPC is an association of the 26 largest state-owned and municipal utilities in the nation and represents the larger, asset-owning members of the public power sector.[2] LPPC members are also members of the American Public Power Associations ("APPA") and own approximately 90% of the transmission assets owned by non-federal public power entities. LPPC members are located throughout the nation, both within and outside RTO boundaries, and they are subject to the Commission's electric reliability regulations and requirements as set forth in Federal Power Act Section 215.

B. The NOPR

The Commission proposes to direct NERC to revise the Critical Infrastructure Protection ("CIP") Reliability Standards to broaden the scope of mandatory reporting under the standards to include "Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS."[3] The Commission further seeks comment on potential

[2] LPPC's members are: Austin Energy, Chelan County Public Utility District No. 1, Clark Public Utilities, Colorado Springs Utilities, CPS Energy (San Antonio), ElectriCities of North Carolina, Grand River Dam Authority, Grant County Public Utility District, IID Energy (Imperial Irrigation District), JEA (Jacksonville, FL), Long Island Power Authority, Los Angeles Department of Water and Power, Lower Colorado River Authority, MEAG Power Nebraska Public Power District, New York Power Authority, Omaha Public Power District, Orlando Utilities Commission, Platte River Power Authority, Puerto Rico Electric Power Authority, Sacramento Municipal Utility District, Salt River Project, Santee Cooper, Seattle City Light, Snohomish County Public Utility District No. 1, and Tacoma Public Utilities.

[3] NOPR at P 4. The currently-effective CIP standards provide that responsible entities must report a Cyber Security Incident only if it has compromised or disrupted one or more reliability tasks of a functional entity. *See* definition of

alternatives to modifying the mandatory CIP reporting requirements, including whether a NERC request for data under Section 1600 of NERC's Rules of Procedure may effectively address the reporting gap the Commission has identified.[4]

The Commission has also proposed to direct NERC to modify the CIP Reliability Standards to specify certain required information to be contained in Cyber Security Incident reports submitted by responsible entities, and to direct NERC to establish a deadline for filing such reports once a compromise or disruption to the Bulk Electric System ("BES"), or attempted compromise or disruption, is identified by a responsible entity.[5]

II. COMMENTS

1. If FERC proceeds, it should be mindful of ongoing information sharing programs, and the potential for a counter-productive effort.

In comments filed contemporaneously, Edison Electric Institute ("EEI") catalogues ongoing efforts aimed at eliciting and processing information related to BES threats and vulnerabilities that is currently being shared through voluntary partnerships and close coordination between responsible entities and the Electricity Information Sharing and Analysis Center ("E-ISAC"), the Department of Energy ("DOE"), and the Department of Homeland Security ("DHS").[6] LPPC agrees with EEI that a new requirement holds the potential to adversely affect the electric subsector's participation in these existing, voluntary industry and government partnerships, and may be counterproductive to the overall goal of sharing timely and actionable threat information. The concerns are threefold: (1) there will be a focus on the compliance burden of new requirements rather than security, with limited intelligence value; (2)

"Reportable Cyber Security Incident," NERC Glossary of Terms Used in the NERC Reliability Standards, *available at* http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[4] NOPR at P 36.

[5] *Id.*, PP 37-42.

[6] *See* Comments of EEI, Docket No. RM18-2 (filed Feb. 26, 2018).

the potential for collection of a great deal of information that is not actionable, potentially obscuring useful information; and (3) diversion of resources from voluntary efforts to share actionable information to compliance management with rigid requirement.

The industry currently coordinates closely with the E-ISAC, DOE, DHS, and the DOE National Laboratories on a variety of programs designed to detect, analyze, and share threat and vulnerability information through voluntary partnerships. Industry executives and their subject matter experts work directly with these entities and, indeed, do report attempted compromises when it is thought that shared information may be of value. Through these partnerships, the expertise and innovation of both industry and government is harnessed to improve threat and vulnerability detection, analysis, and sharing capabilities.[7]

With this as background, there is good reason to be concerned that a rigid mandate may have the effect of requiring responsible entities to shift their resources from efforts to share threat information voluntarily for purposes of security in order to focus on new and broadened compliance activities and reporting requirements. Ongoing and emerging efforts have worked best when they focus on the collection and dissemination of actionable information, while the collection of raw unfiltered data regarding unsuccessful efforts to breach systems may result in a cloud of unusable information. Moreover, a new mandatory requirement may be at odds with the aim of streamlining regulation (the Paperwork Reduction Act). Whatever action FERC takes here, accordingly, must be done with an eye toward causing as little disruption to existing information sharing programs as possible. As discussed below, LPPC believes this may best be

[7] Among the programs in which public power has been directly engaged showing substantial promise is the E-ISAC "Industry Augmentation Program," providing for direct participation of utility employees in E-ISAC operations, simultaneously facilitating industry familiarity with the E-ISAC and encouraging voluntary communication. See: https://www.publicpower.org/periodical/article/nypa-srp-cyber-experts-get-window-how-e-isac-handles-data.

achieved if FERC facilitates a dialogue with NERC and the industry that would help shape any information sharing requirement.

2. Before finalizing any directive, FERC should enable NERC and the industry to work together to establish a sensible threshold for determining which attempts to compromise ESPs and EACMS warrant reporting.

LPPC supports the request made by NERC in comments filed today to work with industry stakeholders to develop "a common threshold" for defining reportable "attempts to compromise:" that will enable NERC and the industry to focus on useful information, without overburdening responsive entities.[8] NERC further indicates that, given the flexibility to appropriately focus its data collection efforts, it would fine tune the focus on EACMS, recognizing that the risk associated with compromise of these devices varies considerably.

A reporting standard that is overly broad in scope could lead to the collection of an overwhelming amount of information, much of which may prove to yield little actionable information, while burdening responsible entities and potentially obscuring more valuable information. Accordingly, LPPC supports NERC's request for needed flexibility in defining the threshold reporting definitions. In addition, LPPC agrees with NERC's request for flexibility to determine the appropriate timeframe within which entities must submit to NERC their full reports regarding Cyber Security Incidents and attempts to compromise. These timelines will very likely affect how this information is used, ranging from early indication of potential attacks to analysis of trends over time.

[8] *See* Comments of NERC, Docket No. RM18-2 (filed Feb. 26, 2018).

3. This process of determining what information may appropriately be the focus of data collection may begin with a FERC-sponsored technical conference.

The Commission, NERC and the industry have productively used technical conferences in order to work toward consensus regarding the state of reliability and the merit of various proposals, including standards and compliance reform. Technical conferences were employed beneficially in discussing the nature and scope of NERC's initially proposed standards, in addressing a host of issues regarding the coordination of FERC's and NERC's respective responsibilities at a critical time in NERC's development, and in addressing the reform of NERC's compliance and monitoring programs.[9]

Here, a technical conference may productively explore the nature and scope of the various programs that currently exist for information sharing regarding threats and the incremental value of any new requirements. The focus of such a conference should be on what information already is being shared and made available currently through voluntary partnerships among responsible entities and various Federal government agencies, and through other channels, as well as how best to fashion a data request to target the collection of information from industry that will add the most value with respect to existing or developing cyber security threats.

4. LPPC Supports the Use of Data Requests through the NERC Rules of Procedure Section 1600 Process, rather than a Reliability Standard.

As an alternative to establishing a broad reporting requirement as part of the NERC Reliability Standards, LPPC supports a more flexible approach to collection of actionable

[9] *See, e.g., Mandatory Reliability Standards for the Bulk-Power System*, Notice of Technical Conference, Docket No. RM06-16 (issued May 31, 2006) (establishing a July 6, 2006 technical conference to consider NERC's proposed Reliability Standards, FERC Staff's Preliminary Assessment of those standards, and related issues); *Mandatory Reliability Standards for the Bulk-Power System*, Notice of Technical Conference, Docket No. RM06-16 (issued Aug. 19, 2010) (establishing a Sept. 23, 2010 technical conference to consider NERC's proposed frequency response-related Reliability Standards).

information through the data request process outlined in NERC ROP Section 1600. In its comments, NERC notes that this data collection process establishes an efficient and mandatory avenue for NERC to collect information from the industry. NERC also provides the assurance – critical to LPPC – that it would work with the industry in shaping the associated data requests.

As noted by NERC, the data request approach offers flexibility that the standards development process does not. As explained by NERC in its comments, the NERC ROP Section 1600 process allows for stakeholder input and FERC staff review of any data request proposed by NERC. Like Reliability Standards, compliance with a NERC data request is mandatory for applicable entities, while the data request procedures specified under ROP Section 1600 also provide a more efficient process to update or revise a data request as needed to respond to rapidly-changing security threats. This flexibility is important, and makes the data request process in NERC ROP Section 1600 a more suitable avenue to gather this information versus data collection through a Reliability Standard.

Further, it seems appropriate to remove the data collection process from the enforcement process associated with mandatory Reliability Standards. Responses to data requests are required, to be sure, but the compliance and sanctions process associated with mandatory standards is a poor fit for the collaborative information sharing process that LPPC believes FERC, NERC and the industry share the goal of promoting.

III. CONCLUSION

LPPC requests that the Commission consider the comments discussed above, as it contemplates the cyber security incident reporting proposals advanced in this docket.

Respectfully submitted,

/s/ Jonathan D. Schneider

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

Counsel to the
Large Public Power Council

Dated: February 26, 2018