ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
213 Market Street
8th Floor
Harrisburg, PA 17101

TEL: 717 237 6000
FAX: 717 237 6019

Deanne M. O'Dell, Esq.
717.255.3744
dodell@eckertseamans.com

February 8, 2023

Via Electronic Filing
Rosemary Chiavetta, Secretary
PA Public Utility Commission
P.O. Box 3265
Harrisburg, PA 17105-3265

Re: Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting – Docket No. L-2022-3034353

Dear Secretary Chiavetta:

Enclosed for electronic filing please find Comments of the Retail Energy Supply Association ("RESA") with regard to the above-referenced matter.

Sincerely,

Deanne M. O'Dell

DMO/lww
Enclosure

Colin Scott, Assistant Counsel, colinscott@pa.gov
Chris Van de Verg, Assistant Counsel, cvandverg@pa.gov
Daniel Searfoorce, Manager – Water, Reliability and Emergency Preparedness Division
dsearfoorc@pa.gov
Michael Holko, Director, Office of Cybersecurity Compliance and Oversight, miholko@pa.gov
Karen Thorne, Regulatory Review Assistant, kathorne@pa.gov

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting	: : :	Docket No. L-2022-3034353

COMMENTS OF
THE RETAIL ENERGY SUPPLY ASSOCIATION

Deanne M. O'Dell, Esquire
Eckert Seamans Cherin & Mellot, LLC
213 Market Street, 8th Fl.
Harrisburg, PA 17108-1248
717 237 6000
dodell@eckertseamans.com

Todd S. Stewart, Esquire
Hawke McKeon & Sniscak LLP
100 North 10th Street
Harrisburg, PA 17101
717.236.1300
tsstewart@hmslegal.com

Date: February 8, 2023

TABLE OF CONTENTS

I. INTRODUCTION....1

II. RESPONSE TO SPECIFIC TOPICS FOR COMMENTS AS IDENTIFIED IN APPENDIX A....3

A. Response to Topic Number 1: Revision of Existing Regulations to Ensure They Address Public Utility Fitness in the Current and Anticipated Future Cybersecurity Threat Landscape....3

B. Response to Topic Number 6: Whether Self-Certification Regulations Should be Applied to Additional Types of Entities Subject to the PUC's Supervision....3

1. RESA Does Not Support Extending Regulations To Suppliers....3

2. If Regulations Extended to Suppliers, Care Must Be Taken To Ensure They Do Not Impose Unnecessary or Costly Requirements....4

C. Response to Topic Numbers 8 and 9: Improving the Self-Certification Form (SCF) Process....6

D. Response to Topic Number 11: Efficacy of Continuing the $50,000 Reporting Threshold....8

E. Response to Topic Number 14: Conflict, Overlap and Redundancy....9

F. Response to Topic Number 15: Other Matters....10

III. CONCLUSION....10

I. INTRODUCTION

By Advanced Notice of Proposed Rulemaking Order ("ANOPR") entered on November 10, 2022, the Commission invited comments to assist in its consideration of whether and how its existing regulations regarding cyber-attack reporting and self-certification (collectively, "existing regulations")[1] should be revised to ensure that they address public utility fitness in the current and anticipated future cybersecurity threat landscape.[2] The Retail Energy Supply Association ("RESA")[3] is an association of diverse competitive energy suppliers devoted to promoting vibrant and sustainable competitive retail energy markets for residential and business customers. Members of RESA include natural gas suppliers ("NGS") and electric generation suppliers ("EGSs") licensed by the Commission, pursuant to the Natural Gas Choice and Competition Act[4] and the Electricity Generation Customer Choice and Competition Act,[5] to sell natural gas supply and electric generation services to retail customers throughout Pennsylvania. NGSs and EGSs are expressly excluded from the definition of "public utility" in the Public Utility Code[6] "except

---

1 52 Pa Code §§ 57.11 (relating to accidents for electricity public utilities); 59.11 (relating to accidents for gas public utilities); 61.11 (relating to accidents for steam utilities): 65.2 (relating to accidents for water public utilities); 101/1-101.7 (relating to public utility preparedness through self certification for jurisdictional utilities); and, 61.45 (relating to security planning and emergency contact list for steam utilities).

2 ANOPR at 1-2.

3 The comments expressed in this filing represent the position of the Retail Energy Supply Association (RESA) as an organization but may not represent the views of any particular member of the Association. Founded in 1990, RESA is a broad and diverse group of retail energy suppliers dedicated to promoting efficient, sustainable and customer-oriented competitive retail energy markets. RESA members operate throughout the United States delivering value-added electricity and natural gas service at retail to residential, commercial and industrial energy customers. More information on RESA can be found at www.resausa.org.

4 66 Pa. C.S. §§ 2201 et seq.

5 66 Pa.C.S. §§ 2801 et seq.

6 66 Pa. C.S. §102 (definition of "public utility").

for limited purposes.[7] As such, the existing regulations do not impose cyber-attack reporting or self-certification filings on the NGSs or EGSs.

RESA appreciates the opportunity to present its views on these important issues. As explained more fully below RESA suggests that the Commission first consider whether the level of interaction between the systems of NGS/EGS and utility systems is sufficient to warrant extending reporting requirements to the NGS/EGS. If the Commission believes that such an extension is needed, RESA urges the Commission to not apply a one-size-fits-all approach and to recognize that certain entities, such as suppliers, pose a substantially lower threat to critical infrastructure than others; and, to impose a level of regulation that is consistent with the levels of risk posed. RESA also is concerned that any standards be industry standards and that the Commission determine the rules and enforce them, rather than allowing each utility to have its own requirements and enforcement mechanisms. RESA also proposes that if the Commission intends to impose any training requirements, which RESA does not believe is necessary for suppliers, that the Commission take a risk-based approach so that levels of training, and the time and expense of the training, are commensurate with the level of risk any particular employee or class of employees pose on the system. In general, RESA proposes what it hopes the Commission will recognize as a common-sense approach that provides the best security without imposing undue burdens and cost.

---

[7] *See HIKO Energy, LLC v. Pa. Pub. Util. Comm'n*, 163 A.3d 1079, 1082 n.1 (Pa. Cmwlth. 2017) (en banc), aff'd, 209A.3d 246 (Pa. 2019); and, *Indep. Oil & Gas Ass'n v. Pa. PUC*, 804 A.2d 693, 697 (Pa. Cmwlth. 2002)

II. RESPONSE TO SPECIFIC TOPICS FOR COMMENTS AS IDENTIFIED IN APPENDIX A

A. Response to Topic Number 1: Revision of Existing Regulations to Ensure They Address Public Utility Fitness in the Current and Anticipated Future Cybersecurity Threat Landscape

RESA supports the Commission's effort to re-evaluate its current cyber-attack reporting and self-certification regulations. As noted in the ANOPR, cyber threats have continuously evolved and increased in number, type, and sophistication since the self-certifications were first drafted in 2005.[8] Similarly, companies have had to continuously evolve to update their internal systems and processes to prepare for such attacks and to address the consequences of such occurrence. RESA members expect continuous evolution as to both the nature of future attacks as well as revisions of internal systems to cope with such attacks. In addition, many RESA members operate in multiple states and, therefore, face a variety of cybersecurity requirements in those states as well as federal requirements. For these reasons, RESA members urge caution regarding revisions to the existing regulations to ensure that: (1) they are in harmony with applicable federal and industry standards; and, (2) they recognize that this area of regulation is an ever moving target and thus use a flexible framework approach than can adapt as circumstances and standards change without the need to revamp the entire structure.

B. Response to Topic Number 6: Whether Self-Certification Regulations Should be Applied to Additional Types of Entities Subject to the PUC's Supervision

1. <u>RESA Does Not Support Extending Regulations To Suppliers</u>

As noted above EGSs and NGSs are not currently subject to the Commission's existing cyber-attack reporting and self-certification regulations. The ANOPR seeks comment on whether the self-certification regulations or revisions thereto should be applied to EGSs and

[8] ANOPR at 10.

NGSs. RESA members do not support applying these additional objections to NGSs and EGSs at this time for several reasons.

First, NGSs and EGSs do not have access to the critical infrastructure that delivers the energy to end user customers. Therefore, any breach of the systems of an NGS or EGS would not directly impact controls or systems for provisioning services. For this reason, RESA members suggest that focus on the utility systems delivering service to end user customers is more appropriate than imposing additional costs on suppliers in this regard.

Second, NGSs and EGSs already comply with industry standards regarding security of their systems. For example, as discussed below in Section C, voluntary compliance standards have been developed regarding the management of customer data and how to proactively safeguard against emerging threats many states, including Pennsylvania, have reporting requirements for reporting data breaches involving personal data.[9] There are also federal reporting requirements such as those maintained by the National Institute of Standards or (NIST). RESA supports a framework that does not specify a specific standard, but rather allows for multiple standards be acceptable to increase flexibility and lower costs. Requiring newly created standards imposes unnecessary development and compliance costs on the suppliers, utilities, and the Commission and imposing strict Commission-made requirements would be unnecessarily redundant and would create additional burdens on suppliers as well as Commission staff who will be tasked with maintaining such requirements.

2. If Regulations Extended to Suppliers, Care Must Be Taken To Ensure They Do Not Impose Unnecessary or Costly Requirements

[9] *Breach of Personal Information Notification Act*, 73 P.S. §2301-2329.

While RESA members do not support the extension of cyber security and self-certification requirements to suppliers, if the Commission elects such path, then consideration must be given to the unique relationship between utilities, suppliers and retail end users.

Importantly, the Commission must ensure that utilities are not given unfair advantages regarding either their ability to dictate terms to the suppliers or to recover the costs of the regulatory requirements from captive ratepayers while forcing suppliers to recover costs through market pricing. To avoid this result, control over any revised regulations must remain with the Commission and be applied, recognizing that different groups of participants engender different levels of risk and thus may warrant greater or lesser intensity of regulation and must be consistent across the Commonwealth. Utilities should not be permitted to establish utility specific regulations or impose requirements that differ from what the Commission requires. Delegating authority to the utilities to implement such measures and/or to enforce the regulatory requirements will further exacerbate the already unlevel playing field as between utilities and suppliers in terms of their prior monopoly status and current exclusive control over the customer billing and information systems. Permitting utilities to impose costly requirements on suppliers could result in driving such competitors from the market to the detriment of end user customers.

In addition, given that the utilities serve all customers in their service territories with distribution service and recover the costs of their service via rate regulation, and not the competitive market, utilities are uniquely positioned to recover regulatory costs from captive ratepayers. Thus, the imposition of the same costly burdens on both the utility and suppliers will have an unequal impact on the ability of suppliers to recover costs. This is because suppliers can only recover costs through the price of service to customers and, if costs are too high, they could

be forced to not offer competitive services. Such result is also harmful for consumers and the competitive market in general.

RESA members also suggest that the Commission consider the level of interaction suppliers may have with the systems of the utilities in determining whether and what type of requirements to impose on the suppliers. Some suppliers, those who do not take title to the energy, may not interact at all with the utility and, therefore, imposing requirements on them may be unreasonable. Other suppliers' interactions with the information systems may be minimal such that any breaches of the supplier's systems are not likely to have widespread end-user customer impacts A one-size fits most approach is not appropriate where the consequences are to impose financial and technical burdens that are not warranted by the facts.

In sum, to the extent the Commission chooses to impose revised cyber security reporting and/or self-certification requirements on suppliers notwithstanding RESA's concerns, the Commission should justify the need for such requirements and share the rationale for any requirements so that comments at future stages can address the underlying rationale as well as the rule. Moreover, any changes should be narrowly tailored, enforced and monitored by the Commission, and apply equally to similarly situated entities.

C. Response to Topic Numbers 8 and 9: Improving the Self-Certification Form (SCF) Process

To the extent the Commission elects to require suppliers to file a self-certification form, RESA members offer a few suggestions. Any form should remain simple and consistent with industry standards without any requirement to file the actual company plans. Since cyber security is a concern among all industries, there are significant resources and information available to guide addressing this issue. The Center for Internet Security ("CIS") is an example of a community-driven nonprofit organization focused on creating standards to proactively

safeguard against emerging threats related to Information Technology.[10] CIS has developed 18 Critical Security Controls to direct companies regarding protocols and measures to consider to protect information technology systems.[11] There are other such organizations with comparable standards. The point is that while the standards set by these organizations may differ, so long as the standards meet the minimum threshold, any such standard should be available. Relying on organizations such as these and the standards they have developed is a reasonable way for the Commission to guide suppliers to compliance with industry best practices for securing their systems.

The Commission could also consider the concept of reducing the periodicity of the reporting requirement, i.e., allowing entities to complete a full report on a longer time schedule, say every three years, but certifying continued compliance on an annual basis without the need to complete the entire form. This could save time and money for all participants including the Commission.

In lieu of the self-certification form, the Commission could also consider allowing suppliers to submit an attestation from a third party entity, certifying that the company is in compliance with the regulations. One example, SOC 2, is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data. The standard is based on security, availability, processing integrity, confidentiality, privacy. An SOC 2 report can be tailored to the unique needs of each organization. Depending on its specific business practices, each organization can design controls that follow one or more principles of trust. These internal reports provide

---

[10] *See* https://www.cisecurity.org/about-us

[11] *See* https://www.cisecurity.org/controls/cis-controls-list

organizations and their regulators, business partners, and suppliers, with important information about how the organization manages its data. There are two types of SOC 2 reports:

- Type I describes the organization's systems and whether the system design complies with the relevant trust principles.
- Type II details the operational efficiency of these systems.

Relying on reputable industry audits and reports such as this is a reasonable way for the Commission to ensure that suppliers are addressing concerns related to cyber security. This type of audit also has the advantage of remaining flexible so that the systems can be analyzed in consideration of the evolving types of known and expected threats. This is but one example of an "industry standard" approach that can allow regulated entities a flexible approach to compliance. There are a number of other such standards that also should be considered, and the Commission could even adopt a process for approval of new and evolving standards to allow maximum flexibility.

Finally, RESA members recommend against requiring the filing of confidential planning reports for an entire industry in one location as doing so creates a potential for catastrophic breach which could provide a statewide roadmap for attackers. While RESA members also do not support mandatory on-site reviews or inspections, members do recognize that if they are required to submit a self-certification then the Commission maintains the ability to conduct an audit if there is a breach or suspected breach. As explained in the previous section, though, any such audit power must remain with the Commission and not be delegated to the utilities.

D. Response to Topic Number 11: Efficacy of Continuing the $50,000 Reporting Threshold

RESA members do not think that suppliers in particular, because breaches of their systems would be limited to customer data, should be subject to reporting that is in addition to

existing reporting requirements under state law. To the extent the Commission believes otherwise, RESA recommends that any new reporting requirements be limited to interruptions in service or that impact such functions as billing. Regardless of the basis for the reporting requirement, however, RESA suggests that it not be tied to a specific dollar amount since dollar impacts are often difficult to calculate and could mask incidents that otherwise should be reported because of their customer impacts. An actual consequence oriented reporting requirement would be more appropriate. For example, did the breach result in access to customer data? Did the breach result in access to connected utility systems? Did the breach result in the interruption of service to customers, etc.? Developing a list of guiding questions would enable suppliers as well as the Commission to determine whether the breach warrants reporting to the Commission. The goal in identifying which breaches should be reported should be to ascertain information about breaches of significance rather than inundating Commission staff with information that has no real impact on systems or customers. Dollar value simply is not an accurate measure of the potential impacts of a breach. Dollar Value, to the extent known, could be reportable if the Commission is interested in maintaining that information, but it is of less value to determining the extent of a breach or the impacts.

E. Response to Topic Number 14: Conflict, Overlap and Redundancy

The Commission asked for comments on the potential for overlap or redundancy with the efforts it seeks to initiate in this ANOPR with ongoing or anticipated rulemakings by other agencies, including the federal government, such as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCIA"). The Department of Homeland Security is expected to shortly begin the process of promulgating regulations at the federal level on incident reporting. The Commission may want to delay proposing rules regarding incident reporting until a later

date when the CIRCIA regulations are at least proposed, to avoid potential overlapping or contradictory requirements.

F. Response to Topic Number 15: Other Matters

One item that is not discussed in the NOPR is the necessity to train employees who use critical IT and OT systems. RESA does not suggest that the Commission impose such requirements because experience shows that human error is the most consistent cause of breaches, and every participant almost certainly has training requirements. To the extent that the Commission believes it necessary to adopt a standards for training of employees who interact with these systems, RESA again suggests a reasoned approach that adapts to the level of access that any particular employee or class of employees may have, to the training requirements that are necessary for those employees or contractors. Considering the negative impacts that excessive training requirements can have on productivity and profitability, RESA recommends requirements that are tailored to threats imposed. And again, standards should be flexible.

III. CONCLUSION

RESA appreciates the opportunity to submit its initial comments to the Commission as the Commission prepares to address regulations aimed at one of the most serious issues facing the utility industry today. RESA supports tailored, and thoughtful regulation that does not impose undue burdens on the resources of those regulated. It is without question that all of the entities to whom these regulations could apply already have systems, protocols and procedures in place to address cyber threats. Requiring such measures is not the primary issue of concern for RESA's members, rather, it is being subject to disparate requirements throughout each supplier's footprint that each require separate certification and notification procedures. To the extent that the Commission can rely upon existing standards and processes, RESA members would save

money and improve efficiency, because members would be faced with fewer permutations to provide for to accommodate Pennsylvania specific requirements.

Respectfully Submitted,

Deanne M. O'Dell, Esquire
PA Attorney ID # 81064
Eckert Seamans Cherin & Mellot, LLC
213 Market Street, 8th Fl.
Harrisburg, PA 17108-1248
717 237 6000
dodell@eckertseamans.com

Todd S. Stewart
PA Attorney ID #75556
Hawke McKeon & Sniscak LLP
100 North 10th Street
Harrisburg, PA 17101
717.236.1300
tsstewart@hmslegal.com

Attorneys for Retail Energy Supply Association

Dated: February 8, 2023