



800 North Third Street, Suite 205, Harrisburg, Pennsylvania 17102

Telephone (717) 901-0600 • Fax (717) 901-0611 • [www.energypa.org](http://www.energypa.org)

February 8, 2023

**VIA ELECTRONIC FILING**

Rosemary Chiavetta, Secretary  
Pennsylvania Public Utility Commission  
Commonwealth Keystone Building  
400 North Street  
Harrisburg, PA 17120

**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 filing please find the comments of the Energy Association of Pennsylvania to the Advance Notice of Proposed Rulemaking Order entered on November 10, 2022 at the above-referenced docket.

Sincerely,

A handwritten signature in black ink that reads "Nicole W. Luciano".

Nicole W. Luciano

Manager, Policy & Research

CC, via email:

Colin Scott, Assistant Counsel, Law Bureau  
Chris Van de Verg Assistant Counsel, Law Bureau  
Karen Thorne, Librarian & Regulatory Coordinator Law Bureau  
Daniel Searfoorce, Manager—Water, Reliability and Emergency Preparedness Division, Bureau of  
Technical Utility Services  
Michael Holko, Director, Office of Cyber Security Compliance and Oversight

**BEFORE THE  
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

Rulemaking to Review Cyber Security  
Self-Certification Requirements and the : L-2022-3034353  
Criteria for Cyber Attack Reporting

---

**COMMENTS OF THE  
ENERGY ASSOCIATION OF PENNSYLVANIA TO  
NOTICE OF PROPOSED RULEMAKING ORDER**

---

**I. INTRODUCTION**

On November 10, 2022 the Pennsylvania Public Utility Commission (“PUC” or “Commission”) entered an Advance Notice of Proposed Rulemaking Order (“ANOPR”) to “review its current regulations relating to cybersecurity.” ANOPR at 1. By “cybersecurity,” the Commission refers to both its cyber attack reporting<sup>1</sup> and self-certification<sup>2</sup> regulations. Primarily, the Commission has opened for public comment “whether the existing regulations are sufficient or if they need to be revised to ensure that they address public utility fitness in the current and anticipated future cybersecurity threat landscapes.” ANOPR at 2. Specifically, a number of years have passed since these regulations were adopted. Since then, cyber threats, protections, standards and responses have evolved. ANOPR at 2-5. While the Commission determines if its regulations should similarly evolve, it has “endeavored not to replicate regulations that were already in place

---

<sup>1</sup> 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, and 65.2 (relating to accidents) for water public utilities.

<sup>2</sup> 52 Pa. Code §§ 101.1–101.7 (Chapter 101, 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.

and required by the federal government or other agencies.” ANOPR at 2. Simultaneously, the Commission acknowledges its vital role in protecting critical utility infrastructure, against reliability threats, across the Commonwealth.

The Energy Association of Pennsylvania (“Association” or “EAP”), a trade association whose members include the major natural gas and electric public utilities operating in the Commonwealth of Pennsylvania, submits these comments on behalf of its electric distribution company (“EDC”) and natural gas distribution company (“NGDC”) members.<sup>3</sup> Individual member companies may also submit additional input on these issues presently before the Commission.

The PUC has asked for feedback on the following issue areas relative to these regulations:

- Updating terms and concepts
- Review of self-certification and/or the role of the Commission in ensuring utilities have adequate cybersecurity plans in place
- The Self-Certification Form (“SCF”) process
- Updating cyber attack reporting regulations
- Potential for merging self-certification and cyber attack reporting regulations
- The cost-benefit analysis of the forgoing items
- Eliminating regulatory duplication and overlap

The ANOPR further breaks down these issue areas into fifteen numbered “topics for comment” attached as Appendix A to the ANOPR. EAP’s comments will follow these main issue areas as outlined by the Commission.

---

<sup>3</sup> EDC Members include: Citizens’ Electric Company; Duquesne Light Company; Metropolitan Edison Company; PECO Energy Company; Pennsylvania Electric Company; Pennsylvania Power Company; Pike County Light & Power Company; PPL Electric Utilities Corporation; UGI Utilities, Inc. (Electric Division); Wellsboro Electric Company; and, West Penn Power Company. NGDC Members include: Columbia Gas of Pennsylvania, Inc.; Pike County Light & Power Company; National Fuel Distribution Corp.; PECO Energy Company; Peoples Natural Gas Company LLC; Philadelphia Gas Works.; UGI Utilities Inc.; and Valley Energy Inc.

Overall, EAP believes the existing regulations requiring self-certification and the specific cyber incident reporting criteria are appropriate and remain relevant and consistent with what other states require. The Commission should maintain a strong focus on: (1) ensuring any changes ultimately made via this process remain aligned with current and future federal regulations/standards; and (2) continuing to avoid unnecessary regulatory duplication. Maintaining these objectives will help the regulations remain broad enough to pertain to all utilities (regardless of size or utility type) while avoiding redundant requirements that would increase regulatory burden for utilities and costs to customers. Existing regulation has struck the correct balance between Commission review of a utility's various emergency plans (including cybersecurity, physical security, business continuity and emergency response), and allowance for utility discretion in the development of those plans and programs.

## **II. COMMENTS**

### **A. Updating Terms and Concepts**

EAP believes that maintaining consistency across definitions is critical, particularly with the goals of avoiding duplication and maintaining uniformity across agencies within Pennsylvania and across states. Adopting new definitions may lead to inconsistent application of the regulations as utilities attempt to interpret broad language to their specific systems and operations. Instead of conforming to non-industry-specific standards, EAP recommends the Commission focus on the information and definitions that are of most interest and actionability by the PUC: items such as interruptions, reliability impacts, or the theft and misuse of Commonwealth residents' information. This narrower focus will allow the Commission to obtain the most pertinent information without creating additional, duplicative reporting that utilities already make to other state and federal agencies.

## **B. Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities**

The ANOPR outlines “five potential regulatory approaches” based on the Commission’s review of what is done on the federal level. ANOPR at 12-13.

1. Similar to existing regulations, require a public utility to self-certify that it has a plan, a program, or both, that complies with criteria set forth in the PUC’s regulations and to report annually to the PUC that such plans and/or programs exist and are updated and tested annually.
2. Require a public utility to self-certify that it has a plan, a program, or both, that complies with an appropriate federal or industry standard and to report annually to the PUC that such plans and/or programs exist and are updated and tested annually.
3. Require a public utility to provide a third-party expert certification that the public utility has a plan, a program, or both, in place that comply with a relevant federal or industry standard appropriate to that utility and to report annually to the PUC that such plans and/or programs exist and are updated and tested annually.
4. Integrate an onsite review of cybersecurity measures, plans, and programs into the PUC’s public utility management audit process and examine cyber security measures, plans, and programs in place as a part of the management audit function.
5. Require a utility to file a confidential copy of its cyber security plans and programs with the PUC and enable the PUC to directly review and comment on the adequacy of such plans and programs and, where deficiencies exist, require conformance with regulatory standards.<sup>4</sup>

EAP believes the Commission should endeavor to maintain its standard of option 1. This is a working process already known to the Commission, staff, and utilities. It is straightforward and easy to implement and execute. Moreover, this option maintains the flexibility needed for utilities to continue aligning their plans with their systems and evolving industry requirements or standards. There would be no additional cost or regulatory burden applicable for utilities to continue with this

---

<sup>4</sup> Numbered list taken from the bullets listed in the ANOPR at pp. 12-13.

approach, which EAP believes continues to meet the Commission's goals. While option 1 is preferred, EAP believes option 2 could be workable with additional clarity and caveats. EAP would not recommend a change to option 2 simply for the sake of change or the appearance of a more rigorous standard. It would need further clarification as to which federal or industry standards are being referred to, and would likely need a carveout for smaller utilities to whom the federal standards do not apply. A blanket adoption as envisioned in the language of option 2 could be costly and time consuming without a clear increase in benefit from option 1.

EAP would caution the Commission against option 3, as this would incur significant costs, particularly for those entities (e.g., small utilities) not currently required to comply with a federal or industry-specific standard. The costs of the assessments themselves can be substantial as well as time consuming for the company to perform. Further, EAP does not believe there is a one-size-fits-all standard by which utilities could be objectively measured via third parties, nor would such a standard be in the best interests of furthering cost-effective and efficient cyber security. Such a requirement would divert essential cyber security resources from systems protection towards compliance. Utilities put significant resources toward protecting against cyber threats with many of those resources guided by the applicable standards utilized (e.g., Cybersecurity and Infrastructure Security Agency ("CISA"), National Institute of Standards and Technology ("NIST"), Transportation Security Administration ("TSA"), North American Electric Reliability Corporation Critical Infrastructure Protection ("NERC CIP"), etc.). Determinations on what certification resources to use (internal or external) are appropriately vested with the utility based on its threat/response experience and the standards utilized.

Option 4 would likewise prove very time-consuming, and may be presently out of reach of Commission staff expertise to perform such an in-depth onsite inspection. To the extent

confirmation of compliance with existing cybersecurity regulations is already taking place in PUC Utility Management Audits, EAP believes this level of review remains reasonable and appropriate.

EAP strongly opposes option 5. A utility's cybersecurity plans and program documents are highly restricted and confidential. No entity, including any federal agencies, presently request or require utilities to provide these confidential documents. The centralized collection by the PUC of regulated utility plans and programs would itself create a high, unnecessary security risk.

With regard to how other states' utility commissions approach cybersecurity fitness, EAP members who have parent or sister companies that operate in other states report many also follow a similar self-certification protocol. EAP refers to individual member company comments about specific examples.

The ANOPR goes on to ask whether changes to the cybersecurity portion of 52 Pa. Code § 101.3 would impact the rules at Chapter 101.<sup>5</sup> EAP believes there are benefits to providing additional clarity regarding the requirement to report (and the process for reporting) cyber incidents as opposed to physical or other incidents. As systems have become inextricably linked, cyber security, physical security, and business continuity are all impacted by any potential change to cybersecurity rules and regulations. However, without a specific proposal from the Commission at this time as to what that would look like, EAP reserves comment.

To perform oversight of cyber security preparedness, EAP recommends that the PUC continue with some form of self-certification that aligns directly with the needs and objectives of the PUC to protect the utility services and information of Commonwealth residents. At the same time, such certification should continue permitting utilities to decide what cyber protocols and resources should be implemented to protect its systems. Continuing this policy of self-certification

---

<sup>5</sup> ANOPR at 13.

allows the PUC to hold a utility responsible to maintain a proper cyber posture and provides a vehicle for addressing utility deficiencies in a reasonable manner without unnecessarily increasing the regulatory burdens and costs.

### **C. Improving the Self-Certification Form (“SCF”) Process**

EAP does not believe there are any major issue with the current SCF and does not recommend any changes. EAP appreciates the burden on Commission staff to secure these documents; however, ensuring that company cybersecurity data is appropriately protected remains critically important. Within each questionnaire is often information that only pertains to one company which that company does not wish to be made public. The PUC should continue to ensure that appropriate processes and controls are in place for protection of these documents.

EAP’s recommendation regarding the SCF is based on current regulations. However, should the form, plan, or reporting requirements become more resource-intensive to complete, the PUC should consider changing the filing to occur every two to three years rather than annually.

### **D. Updating Cyber Attack Reporting Regulations**

The current requirement stating the need to report cybersecurity incidents “immediately” could be specified to allow at least 72-hours to report a confirmed incident as these incidents are generally very complex. At a minimum, any update to the regulations should provide additional detail and clarity concerning under what conditions “immediate” reporting is required, how utilities should report incidents involving information technology (“IT”) systems in a confidential manner, and specifically to whom at the PUC incidents involving IT should be reported. In particular, if there are different guidelines for reporting physical security incidents and cyber security incidents, including to whom at the PUC the incident should be reported, that should be specified in the regulations. The PUC should also consider that many incidents involve both cyber



and physical security and the scope of an incident is not always immediately clear. As such, the PUC Director of Emergency Preparedness would be an appropriate person to notify of any incident related to cyber security, physical security, and/or emergency response.

The Commission should not adopt regulations requiring reports of “attempted compromises” of utility computer systems as has been done in other states and at the NERC CIP<sup>6</sup> level. Reporting “attempted” compromises requires a significant level of subjectivity in determining intent, potential impact, likelihood, etc., that would result in an uneven reporting landscape. It also requires significant internal resource investment to track and analyze various telemetry sources to find things that may require reporting. Other pathways to sharing information with communities and relevant state agencies are more appropriate than via regulation.

The Commission is also seeking comment in this section of the ANOPR with respect to the continuing efficacy of the \$50,000 reporting threshold. EAP agrees that a monetary representation of an attack is difficult to calculate in real time and may ultimately delay reporting if utilities are simultaneously working to address the issue and determine damages. EAP welcomes further discussion on this topic, as it may be more impactful to report those incidents of any monetary value that impact the grid system or customer data.

#### **E. Merging the Self-Certification and Cyber Attack Reporting Regulations**

EAP generally supports any changes that would streamline regulatory language and reduce duplication of the requirements. Reconfiguring these regulations to be contained all within the same chapter would help to ensure that there is consistency. Consolidation would make it easier for the companies to reference and provide feedback when requested. However, such a process should take into consideration the need to remain broad enough to cover all types and sizes of

---

<sup>6</sup> North American Electric Reliability Corporation Critical Infrastructure Protection, referred to in the ANOPR as “CIP Reliability Standards”

public utilities, as well as recognize the relationship between cybersecurity reporting and physical security and emergency response. Without a specific proposal from the Commission at this time as to what that combined language would look like, EAP reserves comment.

#### **F. Cost-Benefit Analysis**

The impact that a cyber incident can have on the Commonwealth is not just financial; it also can result in an operational issue that can leave residents without critical services. Cybersecurity remains a top risk item in every company due to the reputational, financial, operational and safety risks that a breach can bring. Cybersecurity regulations should be evaluated and updated; however, without a specific proposal, EAP reserves comment on the ultimate cost impacts of any change. In general, EAP believes what is currently in place in Pennsylvania is working for the Commission, the utilities, and other stakeholders and any cost analysis would show increased costs for changes to existing rules and regulations without an associated level of benefit or an unclear level of benefit. Changes to cybersecurity regulations carry a high potential for conflict or confusion as these rules are governed by both federal and state entities. Cost savings are currently being realized in the present scheme that avoids duplication of existing federal reporting.

#### **G. Eliminating Regulatory Duplication and Overlap**

As the PUC has recognized, there are numerous federal laws and proposed laws pertaining to cyber incidents and associated reporting requirements. It is in the PUC's best interest to be in alignment with (without duplicating) the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") to ensure that the Commission is receiving the same information that companies are reporting to the federal government. Allowing utilities to self-certify that their plan or program complies with federal and/or industry standards would avoid any duplication issue and

allow for continued flexibility for companies to adapt to how CIRCIA is implemented. EAP urges the Commission to ensure that any Pennsylvania-specific regulations do not duplicate CIRCIA. For smaller utilities, or entities to whom CIRCIA does not apply, EAP encourages the Commission to retain existing processes.

### III. CONCLUSION


EAP appreciates the opportunity to provide comments to this ANOPR issued by the Commission. While noting the minor tweaks or points of clarification detailed above, EAP strongly believes the existing regulations requiring self-certification and the specific criteria for reporting cyber incidents remain broad enough to continue to be relevant, flexible, and appropriate given the ever-changing landscape of cybersecurity and the impacts of evolving threats and attacks.

Respectfully submitted,



---

Nicole W. Luciano  
Manager, Policy & Research  
[nluciano@energypa.org](mailto:nluciano@energypa.org)



---

Terrance J. Fitzpatrick  
President & CEO  
[tfitzpatrick@energypa.org](mailto:tfitzpatrick@energypa.org)



---

Donna M. J. Clark  
Vice President & General Counsel  
[dclark@energypa.org](mailto:dclark@energypa.org)

Energy Association of Pennsylvania  
800 North Third Street, Suite 205  
Harrisburg, PA 17102

Date: February 8, 2023