EAP Energy Association OF PENNSYLVANIA

800 North Third Street, Suite 205, Harrisburg, Pennsylvania 17102
Telephone (717) 901-0600 | Fax (717) 901-0611
www.energypa.org

July 16, 2025

Matthew L. Homsher, Esq., Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor
Harrisburg, Pennsylvania 17120

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

Dear Secretary Homsher:

Enclosed for filing are the comments of the Energy Association of Pennsylvania regarding April 24, 2025 Supplemental Advance Notice of Proposed Rulemaking Order in the above-referenced proceeding.

Sincerely,

Nicole W. Luciano
Director of Policy

Enclosure

cc via email:
Colin Scott, Law Bureau, colinscott@pa.gov
Chris Van de Verg, Law Bureau, cvandeverg@pa.gov
Daniel Searfoorce, Bureau of Technical Utilities Services, dsearfoorc@pa.gov
Michael Holko, Office of Cybersecurity Compliance and Oversight, miholko@pa.gov
Karen Thorne, Law Bureau, 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 ENERGY ASSOCIATION OF PENNSYLVANIA TO APRIL 24th SUPPLEMENTAL ADVANCE NOTICE OF PROPOSED RULEMAKING ORDER

I. INTRODUCTION

On April 24, 2025, the Pennsylvania Public Utility Commission ("PUC" or "Commission) issued a Supplemental Advance Notice of Proposed Rulemaking Order ("Supplemental ANOPR" or "Order") to review its current regulations relating to cybersecurity. The Order supplements the Commission's November 10, 2022, Advanced Notice of Proposed Rulemaking Order in Docket No. L-2022-3034656, *Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting* (Entered on Nov. 10, 2022). This action builds on its November 2022 ANOPR, expanding the discussion in response to:

- Emerging national security threats.
- New federal cybersecurity frameworks and mandates.
- Public comments from utilities, advocacy groups, and industry stakeholders.

The Commission's goal is to modernize, harmonize, and clarify its oversight considering an evolving cybersecurity landscape.

The Energy Association of Pennsylvania ("EAP" or "Association") respectfully submits these comments on behalf of its members. Individual members may also submit company comments. Primarily, EAP's comments address general topics and leave the specific

implementation-implicated questions and issues to individual members as to what is appropriate for each company and its service territory.

II. COMMENTS

EAP and its members appreciate the Commission's proactive effort to update its cybersecurity regulations considering growing cyber threats and evolving federal standards. EAP appreciates that the Commission has thoughtfully considered the feedback provided in our February 8, 2023, comments to the initial ANOPR. The Commission's current approach reflects several key recommendations EAP previously advocated: the need to align with federal standards rather than create duplicative requirements; the focus on maintaining flexibility for utilities of different sizes and risk profiles; and the continued emphasis on self-certification processes. This collaborative approach demonstrates the Commission's commitment to developing practical and effective cybersecurity oversight that serves the interests of both utilities and Pennsylvania consumers while respecting existing federal frameworks.

Our comments reflect consensus feedback across utility sectors, with a shared goal of ensuring robust, scalable, and non-duplicative cybersecurity oversight. Prior to providing specific comments on the items identified in Appendix A to the Order, EAP would like to provide feedback relative to the current state of cybersecurity regulation and the role of the Commission in this effort.

EAP supports the Commission's continued efforts to ensure that the public utilities under its jurisdiction have taken steps to secure their operations from cybersecurity threats. These efforts are consistent with the Commission's mission to ensure safe and reliable service is provided to consumers in the commonwealth. Further, EAP supports the Commission's objective to modernize cybersecurity oversight, but again emphasizes the importance of maintaining a

flexible, risk-based framework that avoids redundancy with existing federal regulations. To the extent that utilities are currently subject to federal cybersecurity requirements, the Commission should defer to the associated federal agency. Indeed, if the Commission were to institute separate but similar reporting requirements – instead of accepting current federal standards – it would risk duplicative burdens, conflicting deadlines, and misaligned definitions. For those utilities that are not subject to federal cybersecurity requirements, the Commission can adopt a review process commensurate with their risk profile without applying overly rigid program elements. For this reason, EAP recommends that the Commission adopt a deferential approach in evaluating utility efforts to address cybersecurity.

A. Cyber Security Fitness Standards
(Appendix A, Questions 1 – 4)

1. Use of Established Standards

EAP agrees that utilities should maintain robust cybersecurity programs but recommends allowing utilities to satisfy compliance obligations by aligning with widely accepted frameworks where such requirements already exist. Specifically, many EAP members already conform to federal or industry cybersecurity standards (e.g., NIST CSF, TSA Pipeline Security Guidelines, FERC/NERC CIP for transmission). Accordingly, utilities should have the flexibility to adopt other industry-standard frameworks that reflect their operations and risk profile. Absent required adoption of another standard, utilities cybersecurity programs should be broadly aligned to the NIST CSF or another structure that can be mapped, as necessary for oversight, to the NIST CSF.

2. Classifications and Waivers

While the proposed classifications seek to recognize differences amongst utilities due to the number of customers served or critical infrastructure operated, EAP suggests that the proposed classifications are not necessary as most frameworks already recognize the entity's risk

profile and program maturity in applying the underlying guidelines.[1] Again, EAP and its members support the Commission maintaining a flexible, risk-based framework. This framework is achievable, without the need of the proposed tiers, by allowing Pennsylvania's utilities to continue to tailor their programs to their operations, risk tolerance, and maturity and in alignment with NIST CSF and other recognized systems.

3. Compliance and Confidentiality

EAP recommends a recurring self-certification process with the option for Commission staff to inspect plans and annual certifications at utility facilities. Certification documents should not require disclosure of detailed architecture or system-level data. Annual certifications should be treated as Confidential Security Information ("CSI")[2]. EAP believes that the PUC's current self-certification form is consistent with this objective.

EAP strongly emphasizes that all cybersecurity-related documents – including incident reports, security plans, vulnerability assessments, and compliance certifications – constitute CSI, which should not be filed with or stored at the Commission. These documents contain sensitive operational details, system vulnerabilities, network configurations, and security protocols that, if compromised, could facilitate cyberattacks against Pennsylvania's critical utility infrastructure. Instead, EAP recommends that the Commission adopt an on-site review protocol whereby Commission staff can inspect cybersecurity documents at utility facilities under appropriate confidentiality agreements and security controls. This approach allows the Commission to fulfill its oversight responsibilities while maintaining the security of sensitive information within utilities' existing protected environments. Such on-site reviews provide the Commission with

[1] Should the Commission find classifications necessary, EAP believes Class 3 as proposed would be appropriate for most, if not all, utilities, particularly small utilities.
[2] Public Utility Confidential Security Information Disclosure Protection Act, 35 P.S. § 2141.1—2141.6 (CSI Act).

necessary visibility into utility cybersecurity preparedness without creating additional attack vectors through document transmission or centralized storage. This methodology aligns with established practices in other regulated industries where sensitive security information requires direct oversight without compromising operational security through unnecessary document proliferation.

B. Cyber Incident Reporting
(Appendix A, Questions 5-8)

1. Reporting Thresholds

The Commission's mission to ensure safe, reliable utility service differs from CISA's real-time threat aggregation under CIRCIA. The CISA NOPR to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), has significant issues[3] and Commission should not seek to replicate or rely on CIRCIA for its regulatory oversight needs. The PUC has acknowledged, appropriately, that its purview must necessarily be narrower than CISA's under CIRCIA. To that end, EAP requests that the Commission remove its proposed requirement that utilities report on "imminent" threats, which exceeds the current requirement proposed by CISA.

In addition, EAP strongly opposes any requirement for utilities to broadly report attempted cybersecurity breaches to the Commission. As we noted in our February 2023 comments, such reporting requirements would create significant operational and regulatory challenges that ultimately undermine rather than enhance cybersecurity protection

Modern utility systems face thousands of attempted intrusions daily through automated scanning, phishing attempts, and other routine cyber activities. Requiring reporting of every

[3] For example, see the comments of the Edison Electric Institute filed on July 3, 2024.

"attempt" would inundate Commission staff with largely irrelevant information while diverting critical cybersecurity personnel from actual system protection to compliance reporting. This volume would render the reporting system ineffective for identifying genuine threats requiring Commission attention.

Further, determining what constitutes a reportable "attempt" requires substantial subjective judgment regarding intent, sophistication, and potential impact. This subjectivity would create an uneven reporting landscape where similarly situated utilities might interpret identical events differently, undermining the Commission's ability to assess comparative cybersecurity postures across the commonwealth.

Threat analytics, both in unique and aggregate cases, are already well-established by the commercial security industry at cost-effective pricing, through various sector-specific security organizations (e.g., Electricity Information Sharing and Analysis Center ("E-ISAC"), Oil and Natural Energy Information Sharing and Analysis Center ("ONE-ISAC"), Water Information Sharing and Analysis Center ("WaterISAC"), etc.), as well as through public sources including the Department of Homeland Security CISA even absent the rulemaking regarding CIRCIA. The Commission establishing its own capability would be duplicative and not cost-effective for the commonwealth.

In addition, utilities already report successful breaches and significant incidents that impact operations or customer data. The Commission's legitimate regulatory interest lies in security compromises that affect service reliability or customer protection, not speculative threats that existing security measures successfully repelled.

EAP appreciates the Commission's commitment to step in to fill the gap identified[4] while not creating new requirements not already imposed by federal agencies that have primary jurisdiction and expertise over this area. The Commission's role should remain focused on the cybersecurity impacts to the delivery of safe and reliable utility service. Therefore, EAP requests that the Commission's regulatory efforts over cybersecurity threats to Pennsylvania utilities remain focused on incidents with demonstrated impact on Pennsylvania utility operations or customers, allowing utilities to concentrate their cybersecurity resources on prevention rather than exhaustive attempt documentation.

2. Federal Alignment

In response to Question 6, EAP recommends that the appropriate roles for the Commission are:

- (c) Provision of early warnings;
- (e) Supporting federal resilience efforts; and
- (f) Information sharing among stakeholders

As there are several federal regulatory frameworks in place that address cybersecurity regulation, EAP recommends that the Commission not engage in technical threat analysis or direct incident response. Instead, the Commission should defer to the existing federal network, which is better suited to sector-specific federal agencies.

The Commission should accept reports submitted to TSA, DOE, or CISA to satisfy its requirements where applicable. Utilities with no critical infrastructure or those subject to

[4] As stated in the Supplemental ANOPR, "[T]here are significant gaps in the cybersecurity standards regimes maintained by federal sector specific agencies. For example, the United States Federal Energy Regulatory Commission (FERC) implemented cybersecurity reliability standards, but these only applied to the bulk power system, not local distribution networks." p.13.

comprehensive federal regulation (e.g., TSA-regulated pipelines) should be exempt from duplicative reporting. As stated *supra*, EAP recommends that all cybersecurity documents remain classified as CSI and not be filed with or stored at the Commission due to security risks. Instead, Commission staff should conduct on-site reviews at utility facilities under appropriate confidentiality agreements.

C. Regulatory Duplication and Jurisdictional

As noted previously, there already exists an extensive federal regulatory framework under which many Pennsylvania utilities are already subject to rigorous federal cybersecurity regulation, including:

- **FERC/NERC CIP Standards** – Electric utilities connected to the bulk power system.
- **TSA Pipeline Security Directives** – Large gas and hazardous liquid utilities.
- **CISA/CIRCIA Requirements** – Critical infrastructure operators.

These frameworks cover assert classification, vulnerability assessments, penetration testing, incident response, and personal training – all with enforceable requirements and federal oversight. Rather than seek to institute new reporting requirements, the Commission should avoid duplicating federal mandates and instead focus on facilitating coordination with federal agencies and monitoring high-level compliance indicators, not prescriptive controls.

D. General Issues

EAP supports eliminating cybersecurity provisions from Chapter 101. Relying on the existing federal cybersecurity framework and requiring Pennsylvania utilities to demonstrate

compliance with equivalent federal standards will aptly allow the Commission to meet its obligations to ensure safe, reliable utility service in Pennsylvania.

Additionally, EAP respectfully requests that the Commission consider the significant costs associated with any enhanced cybersecurity reporting requirements and provide appropriate cost-recovery mechanisms for utilities to recover these expenses. Cybersecurity investments and compliance activities represent prudent operational expenses necessary to maintain safe and reliable utility service, directly benefiting customers through improved system security and service continuity. Enhanced reporting requirements would necessitate additional staffing, specialized training, system upgrades, third-party assessments, and ongoing compliance monitoring – all of which represent legitimate utility operating costs. Accordingly, utilities should be permitted to recover reasonable and prudent cybersecurity compliance costs through appropriate rate recovery mechanisms, ensuring that enhanced security measures do not create financial disincentives for utilities to maintain robust cybersecurity programs.

E. Conclusion

EAP and its member companies remain committed to maintaining robust cybersecurity programs while working collaboratively with the Commission to develop effective oversight mechanisms. We applaud the Commission's efforts in this Supplemental ANOPR to work toward adopting a framework that recognizes existing federal standards, avoids duplicative reporting requirements, and respects the sensitive nature of cybersecurity information.

While noting the suggestions 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. The

Commission can achieve its cybersecurity objectives while supporting utilities' ability to effectively protect Pennsylvania's critical infrastructure by maintaining focus on security incidents rather than attempted breaches, aligning with federal frameworks, and implementing practical oversight procedures.

Respectfully submitted,

Andrew S. Tubbs
President & CEO
(ID # 80310)
atubbs@energypa.org

Nicole W. Luciano
Director of Policy
nluciano@energypa.org

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

Date: July 16, 2025