Essential™
Providing natural resources for life.

VIA E-FILING

July 16, 2025

Matthew L. Homsher, 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 Homsher:

Aqua Pennsylvania, Inc. ("Aqua") and the Peoples Natural Gas Company LLC ("Peoples") are submitting Joint Comments in response to the Pennsylvania Public Utility Commission's Supplemental Advanced Notice of Proposed Rulemaking Order ("ANOPR") regarding the Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting entered on April 24, 2025 at the above Docket.

If you have any questions regarding this filing, please contact Alex Stahl at 610-645-1130 or by email at astahl@aquaamerica.com, or Meagan Moore at 412-208-6527 or by email at Meagan.Moore@peoples-gas.com.

Sincerely,

Alexander R. Stahl
Regulatory Counsel

Meagan Moore
Senior Attorney

Enclosure

cc: Colin Scott, Law Bureau (via email)
Chris Van de Verg, Law Bureau (via email)
Daniel Searfoorce, Bureau of Technical Utility Services (via email)
Michael Holko, Office of Cybersecurity Compliance and Oversight (via email)
Karen Thorne, Law Bureau (via email)

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

JOINT COMMENTS OF AQUA PENNSYLVANIA, INC. AND PEOPLES NATURAL GAS COMPANY LLC ON THE ADVANCED NOTICE OF PROPOSED RULEMAKING ORDER

AND NOW COMES Aqua Pennsylvania, Inc. ("Aqua") and Peoples Natural Gas Company LLC ("Peoples") (together, the "Joint Commenters"), pursuant to the Supplemental Advanced Notice of Proposed Rulemaking Order ("Supplemental ANOPR") published in the Pennsylvania Bulletin on April 24, 2025, to file these comments with the Pennsylvania Public Utility Commission ("PUC" or the "Commission").

I. INTRODUCTION

On April 24, 2025, the Commission issued a Supplemental ANOPR to review its current regulations relating to cybersecurity. The Supplemental ANOPR 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 public utilities, advocacy groups, and industry stakeholders.

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

Aqua and Peoples appreciate the opportunity to participate in this proceeding and the Commission's continued focus on cybersecurity. The Joint Commenters have reviewed the Supplemental ANOPR and have general comments and recommendations before providing answers to the Commission's questions.

II. COMMENTS

At the outset, the Joint Commenters highlight the balance between regulatory oversight of this critical part of providing safe and reliable service and 1) the rapid and every changing cyber security space and 2) already required rules and regulations in place. The Joint Commenters advocate for an incremental and deliberate approach to this highly complicated, ever changing and fluid space.

The Joint Commenters' primary recommendation would be first to review the current regulations in place and add more key questions for self-certification. This could be a first and important step in addressing cybersecurity. A whole new regulation may not be necessary at this time. Self-certification was the key avenue for Commission review in the current regulations that were promulgated as a result of the September 11, 2001 attacks. That method has proved to be a valid method. The Joint Commenters understand that in many PUC audits for the larger companies, the auditors review these confidential documents and processes. This approach has struck an appropriate balance between addressing changing rules and regulations and allowed the Commission first hand review of these documents that are considered confidential security information.

The Joint Commenters further recommend a stakeholder conference so that our experts can discuss our concerns and recommendations in greater detail.

The Joint Commenters appreciate that the Commission has considered the feedback provided in the comments to the initial ANOPR. This collaborative approach demonstrates the Commission's commitment to developing practical, effective cybersecurity oversight that serves the interests of both public utilities and Pennsylvania consumers while respecting existing federal frameworks.

The Joint Commenters support the Commission's objective to modernize cybersecurity oversight but impress the importance of maintaining a flexible framework that avoids redundancy with existing federal regulations. Duplicate reporting requirements are inefficient in that multiple agencies review and comment on required filings. Multiple staff both internally and externally are then required to respond to, meet and explain and connect these various requirements. All of this is borne on our ratepayers. Wherever possible, duplicate reporting requirements should be avoided. To the extent that public utilities are currently subject to federal cybersecurity requirements, the Commission should defer to the associated federal agency requirements. Not doing so would risk duplicative burdens, conflicting deadlines, and misaligned definitions. The Joint Commenters' responses to the Supplemental ANOPR questions continue below.

A. Use of Established Standards

In response to the questions posed in the Supplemental ANOPR, the Joint Commenters agree that public utilities should maintain vigorous cybersecurity programs, but recommend allowing utilities to maintain compliance with widely accepted frameworks where they already exist. The Joint Commenters recommend that the PUC require the jurisdictional utilities to self-certify whether they conform to a specific standard. The self-certification can be reviewed upon

request. After a period of time, if a specific standard or framework is being utilized, it can be addressed through further modification to the self-certification. The Joint Commenters note that the National Institute of Standards and Technology ("NIST") Cybersecurity Risk Framework ("CSF") is more of a structured, flexible, and repeatable approach for organizations to manage cybersecurity risks. It is relevant for critical infrastructure but is designed to be adaptable for organizations of all sizes. If the Commission requires this, the Joint Commenters recommend starting with the less prescriptive model of NIST CSF prior to requiring organizations to conform to NIST 800-53.

B. Utility Classifications and Waivers

All public utilities should be treated similarly regardless of size or capability. We strongly recommend that the Commission include a provision allowing utilities to request a waiver from specific reporting or certification requirements, provided they can demonstrate strict adherence to equivalent or more rigorous cybersecurity frameworks. The public utility should be required to clearly define the framework(s) it adheres to and demonstrate how those standards meet or exceed the intent of the PUC's requirements.

For example, electric utilities subject to the North American Electric Reliability Corporation Critical Infrastructure Protection ("NERC-CIP") standards already operate under a highly prescriptive and enforceable cybersecurity regime. Requiring duplicative reporting to the PUC would not enhance security and could divert resources from operational response.

A waiver mechanism would allow the Commission to maintain oversight while recognizing the maturity and rigor of existing sector-specific frameworks.

As recommended previously, the Joint Commenters continue to advocate for self-certification. Frameworks will evolve over time, and so it does not make sense to promulgate

prescriptive regulations for this matter. The review of standards and frameworks can be upon request, in base rate cases, or in a management audit. Substantial updates—such as the transition from NIST CSF 1.1 to 2.0—should include at least a one-year implementation moratorium before becoming mandatory, to allow organizations adequate time for alignment and adoption.

While the proposed classifications seek to recognize differences amongst utilities because of the number of customers served or critical infrastructure operated, the Joint Commenters ultimately believe the proposed classifications are not necessary. Again, the Joint Commenters support the Commission maintaining a flexible, risk-based framework. This framework is achievable, without the need of proposed tiers, by ensuring that Pennsylvania's public utilities tailor their programs to their operations, risk tolerance, and maturity and adhere via alignment with NIST CSF.

C. Compliance and Confidentiality

The Joint Commenters recommend a periodic self-certification process with the ability for Commission staff to review and inspect plans at public utility facilities. Certification documents should not require disclosure of detailed architecture or system-level data.

The annual cybersecurity certification should be treated as confidential information. Public disclosure of an organization's adherence to a cybersecurity standard could inadvertently expose it to targeted attacks by threat actors. Such disclosures may signal potential weaknesses in cybersecurity posture or compliance readiness, making organizations more vulnerable. To mitigate this risk, certification status should be shared only with authorized regulatory bodies and not made publicly accessible. The Joint Commenters instead recommend that the Commission enact an on-site review standard whereby Commission staff can review cybersecurity documents at the utility's secure location under confidentiality agreements. These in-person reviews provide the

Commission with access to utility cybersecurity preparedness without creating additional attack vulnerabilities and is consistent with established practices in other regulated industries where sensitive security information requires direct oversight.

D. Cyber Incident Reporting & the PUC's Role

The proposed cybersecurity incident reporting requirements outlined in the PUC's Supplemental ANOPR raise important considerations regarding regulatory overlap with federal mandates—specifically those under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), administered by the Cybersecurity and Infrastructure Security Agency ("CISA"). We respectfully submit that the Commission should carefully evaluate the potential for regulatory duplication and consider the following:

- Redundancy in Reporting Obligations: CISA's forthcoming rules under CIRCIA will require covered entities to report covered cyber incidents within 72 hours and ransomware payments within 24 hours. These requirements are designed to support national threat awareness and response coordination. If the PUC imposes parallel reporting obligations without harmonization, public utilities may face duplicative compliance burdens that divert resources from actual incident response.
- Lack of Interagency Coordination: CISA's current framework does not contemplate direct information sharing with state commissions. This gap increases the likelihood that public utilities will be required to submit similar or identical reports to multiple agencies, each with different formats, timelines, and thresholds.

By aligning with federal standards and leveraging existing reporting mechanisms, the Commission can enhance cybersecurity oversight while minimizing unnecessary regulatory friction.

The Joint Commenters strongly oppose any requirement for utilities to broadly report attempted cybersecurity breaches to the Commission. Utilities experience thousands of cyberattack attempts daily. Requiring utilities to report each and every attempt is untenable for operational staff for both the utility and the PUC. This level of compliance reporting would take up the time of cybersecurity staff when they should instead focus on performing the critical system protection. To put it simply, if every attempt is reportable, then the actual critical threats would not receive proper attention from the PUC. Public utilities already report breaches and major incidents that impact operations or customer data. The Joint Commenters contend that the Commission's chief regulatory concern should be limited to actual security incidents that affect service reliability or customer protection, not attempts that are successfully thwarted.

The Joint Commenters believe the PUC's roles should relate to the following, which were provided in the Supplemental ANOPR:

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

There are already several federal regulatory frameworks in place that address cybersecurity regulation, as such, the Commission should defer to the existing federal framework which is better suited to sector-specific federal agencies.

The Commission should accept cyber incident reports submitted to federal agencies to satisfy its requirements, where applicable. Utilities with no critical infrastructure should be exempt from duplicative and burdensome reporting. The Joint Commenters believe all cybersecurity documents should remain as confidential security information and not be filed with or stored at

the Commission due to security risks. Instead, as previously stated, the Commission staff should conduct on-site reviews at public utility facilities under appropriate confidentiality agreements.

E. General Issues

The Joint Commenters support eliminating cybersecurity provisions from Chapter 101 of the Commission's regulations. Relying on the existing federal cybersecurity framework and requiring Pennsylvania public utilities to demonstrate compliance with equivalent federal standards will allow the Commission to meet its obligations to ensure safe, reliable public utility service in Pennsylvania.

The Commission should also consider the significant costs associated with any increased cybersecurity reporting requirements and provide and/or allow for appropriate cost-recovery mechanisms to recover these expenses. It should go without saying that investments in cybersecurity compliance are prudent operational expenses necessary to maintain safe and reliable public utility service. These investments directly benefit customers through improved system security and service continuity.

III. CONCLUSION

The Joint Commenters appreciate the opportunity to provide input and look forward to continued collaboration on this important issue.

The Joint Commenters remain committed to maintaining robust cybersecurity protocols and safeguards and working collaboratively with the Commission to develop effective oversight mechanisms. The Commission can achieve its cybersecurity objectives while supporting public utilities' ability to effectively protect Pennsylvania's critical infrastructure by aligning with federal frameworks already in place, continuing self-certification and practical oversight, and maintaining focus on actual security incidents rather than attempted breaches.

Respectfully submitted,

Respectfully Submitted,

Alexander R. Stahl
Regatory Counsel Aqua Pennsylvania, Inc. 762 W. Lancaster Ave. Bryn Mawr, PA 19010 Phone: 610-645-1130
astahl@aquaamerica.com

Respectfully Submitted,

Meagan Moore
Senior Attorney
Peoples Natural Gas Company LLC
375 North Shore Drive
Pittsburgh, PA 15212
Phone: 412-208-6527
Meagan.moore@peoples-gas.com