PENNSYLVANIA AMERICAN WATER

Erin K. Fure
Director, Corporate Counsel
852 Wesley Drive | Mechanicsburg, PA
17055 Phone: 717-550-1556
erin.fure@amwater.com

July 16, 2025

VIA eFiling

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

Re: Supplemental Advance Notice of Proposed Rulemaking Order

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 with the Pennsylvania Public Utility Commission are the Comments of Pennsylvania-American Water Company on the above-referenced Rulemaking.

These Comments are being provided in Word®-compatible format to the contact persons listed below.

If you have any questions, please contact me.

Sincerely,

Erin K. Fure

Enclosure

cc: Karen Thorne, Law Bureau w/Enc. **VIA** Email

Contact Persons w/Enc. **VIA** Email:

Colin Scott, Assistant Counsel, Law Bureau
Chris Van de Verg, Deputy Chief Counsel, Law Bureau
Daniel Searfoorce, Manager—Water, Reliability and Emergency Preparedness Division, Bureau of Technical Utilities Services
Michael Holko, Director, Office of Cybersecurity Compliance and Oversight

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 PENNSYLVANIA-AMERICAN WATER COMPANY

I. INTRODUCTION

Pennsylvania-American Water Company ("PAWC" or the "Company") submits these Comments in response to the Supplemental Advance Notice of Proposed Rulemaking Order ("Supplemental ANOPR" or "Order") entered by the Pennsylvania Public Utility Commission ("PUC" or the "Commission") on April 24, 2025 at the above-captioned docket and published in the Pennsylvania Bulletin on May 17, 2025. The Supplemental ANOPR solicits comments from stakeholders regarding whether the existing regulations are sufficient or if they need to be revised to ensure they address public utility fitness in the current and anticipated future cybersecurity threat landscapes. The Supplemental ANOPR included for stakeholder consideration both a list of questions set forth in its Appendix A and staff working proposals set forth in its Appendix B. In the following section, PAWC will provide its comments in response to both Appendix A and Appendix B.

II. COMMENTS IN RESPONSE TO APPENDIX A

In this section PAWC will provide comments in response to the questions listed in Appendix A of the Supplemental ANOPR. The questions are reproduced in bold text in this section for ease of reference.

A. Questions Related to Cybersecurity Fitness Standards

1. **Should the Commission require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks such as NIST Cybersecurity Risk Framework, NIST Special Publication 800-53, and/or NIST Special Publication 800-82?**

The Company believes that the Commission should require jurisdictional utilities to maintain cybersecurity programs and plans that conform to the specific standards and frameworks. Specifically, the Company recommends that the Commission require jurisdictional utilities to maintain cybersecurity programs and plans that conform to the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF") 2.0[1] and NIST Special Publication 800-61[2] (Incident Response Recommendations).

2. **If the Commission does require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks:**

   a. **Should the Commission consider the extent and burden of the requirement(s) in relation to the size of the utility? If so, what criteria might the Commission use to classify utilities for purposes of differentiating their respective obligations when it comes to a utility's size and capabilities**?

While it may be appropriate for the Commission to consider the burden of requirements in relation to the size of a regulated utility, communities served by smaller utilities should be entitled to at least a base standard of cybersecurity. PAWC submits that a threshold requirement should

[1] https://doi.org/10.6028/NIST.CSWP.29
[2] https://doi.org/10.6028/NIST.SP.800-61r3

be applied to all utilities regardless of size. Therefore, the Commission should articulate minimum requirements that apply to all jurisdictional utilities' cybersecurity programs regardless of size.

In terms of classifying utilities for the purpose of differentiating their cybersecurity obligations, the Company suggests that the Commission retain consistency with its existing regulations. For example, in 52 Pa. Code § 65.16 provides:

> (a) a public utility having annual operating revenue of $750,000 or more (average of the last 3 consecutive years) shall keep its accounts in conformity with the most recent *Uniform System of Accounts for Class A Water Utilities* prescribed by the National Association of Regulatory Utility Commissioners (N.A.R.U.C.).
>
> (b) a public utility having annual operating revenue of $150,000 or more but less than $750,000 (average of the last 3 consecutive years) shall keep its accounts in conformity with the most recent *Uniform System of Accounts for Class B Water Utilities* prescribed by N.A.R.U.C.
>
> (c) a public utility having annual operating revenue of less than $150,000 (average of the last 3 consecutive years) shall keep its accounts in conformity with the most recent *Uniform System of Accounts for Class C Water Utilities* prescribed by N.A.R.U.C.

Additionally, under 52 Pa. Code § 65.55, "a Class A public utility or authority shall file a [lead service line replacement] program within 1 year of the effective date of this section. A Class B public utility, Class C public utility, or municipal corporation shall file a [lead service line replacement] program within 2 years of the effective date of this section." In order to ensure conformity among the Commission's regulations, the Company suggests that to the extent utilities are already divided into classes under existing regulations, these same classes be maintained in the regulations concerning cybersecurity.

b. Should the Commission specify the criteria it would consider in a petition to waive such requirements?

PAWC is in favor of the Commission articulating the criteria it would consider in a petition to waive cybersecurity requirements. Filings with the Commission take up time and resources,

both for the utility and the Commission itself. Having clear guidance from the Commission will assist utilities in evaluating whether or not they wish to pursue a waiver. Specifying criteria for evaluating petitions for waiver of requirements should also lead to conformity among filings, which would assist Commission review.

c. Should the Commission enable utilities to request waivers for the use of cybersecurity programs and plans that utilize equal or stricter standards and frameworks?

If a utility's cybersecurity programs and plans use equal or stricter standards and frameworks than the Commission's regulations, it seems that the standards set forth by the regulations would have been met or exceeded. The Company suggests that in lieu of a waiver requirement, the Commission include in its regulations a method by which the utility may aver that its cybersecurity programs and plans use equal or stricter standards and frameworks than the Commission's regulations require, and that such averment may be accepted by the Commission as proof of the utility's compliance with the applicable regulation. The utility should be required to provide the mappings from the standards they use to demonstrate that standards and frameworks for their cybersecurity program/plan provide equal or heightened protection than the standards set forth by the Commission.

PAWC is not opposed to the suggestion of allowing the Commission to enable utilities to request waivers for the use of cybersecurity programs and plans that utilize equal or stricter standards and frameworks. If the standard or framework is equal to or stricter than the requirements set by the Commission, the public interest is served by ensuring that the utility not only meets, but may also exceed, the protections the Commission deems necessary. However, the Company views the use of waivers as creating more burdensome requirements than may otherwise be necessary given the alternative proposed by PAWC in the preceding paragraph.

d. Should the Commission enable smaller utilities with less critical infrastructure to request waivers to specific standards and frameworks if they can demonstrate that they do not apply to them?

PAWC does not oppose making the option of requesting a waiver available to smaller utilities if they can demonstrate a specific standard or framework would be inapplicable; however, as indicated in response to Question 2.a above, the Commission should establish basic standards that apply to all utilities regardless of size so that all customers receiving public utility services within the Commonwealth are guaranteed some form of cybersecurity protection.

e. How should the Commission account for changes and updates to those standards and frameworks over time?

The Company believes it is reasonable to provide a three-month review period following updates to any standards once fully adopted. After the three-month review period expires, each utility should act within a reasonable timeline to make changes to their program to meet the revised standards and frameworks.

f. How should the Commission confirm compliance with those requirements?

PAWC suggests that requiring utilities to submit an annual self-certification to the Commission confirming compliance with these requirements would be appropriate. Additionally, the Commission's Bureau of Audits should review a utility's cybersecurity program and plan as part of any management and operational audit that is conducted.

g. How should the Commission enforce those requirements in the event of violations?

PAWC posits that the Commission already has many tools at its disposal to enforce its regulations (e.g. the imposition of civil penalties under 66 Pa. C.S. § 3301).

3. Should an annual certification by a public utility that it adheres (or does not adhere) to a specific cybersecurity standard be considered confidential security information (CSI) pursuant to Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act, 35 P.S.§ 2141.1—2141.6 (CSI Act).

"Confidential security information" is defined in 35 P.S. § 2141.2 as "information contained within a record maintained by an agency in any form, the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, public property or public utility facilities." An annual certification in which a utility acknowledges that it does not adhere to a specific cybersecurity standard appears to meet that definition. At a minimum, PAWC believes that an annual certification disclosing whether a utility does or does not adhere to a specific cybersecurity standard should be considered confidential information, similar to the Self Certification Form required under 52 Pa. Code § 101.4, and the Commission should explicitly acknowledge its confidential designation in regulations, similar to the acknowledgment found in 52 Pa. Code § 101.5 regarding the confidential nature of the Self Certification Form.

4. If an annual certification should be considered CSI, what procedures should the Commission follow to securely accept electronic filing of certifications consistent with the CSI Act?

PAWC suggests that the Commission look to other jurisdictions for methods to securely accept electronic filings consistent with the CSI Act. For example, the New Jersey Board of Public Utilities uses the New Jersey Cybersecurity and Communications Integration Cell which provides a portal through which sensitive utility information can be collected.

B. Questions Related to Cyber Incident Reporting

5. Are the purposes and design for cyber incident report collection stated by CISA, NOPR at Section III.C. ("Purpose of Regulation"), substantially the same as the Commission's statutory role in ensuring that jurisdictional utilities provide reasonably adequate, reliable, continuous and safe service to the public?

The Commission's role in ensuring jurisdictional utilities provide reasonably adequate, reliable, continuous and safe service to the public aligns to some extent with the purposes and design for cyber incident report collection stated by CISA, namely, to enhance the public health and safety. However, the purposes of cyber incident report collection by CISA also include trend and threat analysis, vulnerability and mitigation assessment, and incident response and mitigation, which as discussed below, are areas to which the Commission's role does not appear to extend.

6. Identify any role you believe the Commission has to play in each of the following areas:

a. Trend and threat analysis (i.e., the performance of cybersecurity threat and incident trend analysis and tracking, to include the analysis and identification of adversary tactics, techniques, and procedures (TTPs)).

For the area of trend and threat analysis, the Company believes the Commission's primary role would be the dissemination of information. While it is not the Commission's position to generate intelligence, the Commission would be a resource to utilities in disseminating intelligence from the Federal Bureau of Investigation ("FBI"), National Security Agency ("NSA"), and Department of Homeland Security ("DHS").

b. Vulnerability and mitigation assessment (i.e., the identification of cyber vulnerabilities and the assessment of countermeasures that might be available to address them).

CISA offers a Cyber Hygiene ("CyHy") program which provides vulnerability and mitigation assessment. PAWC does not see a need for the Commission to extend its resources to the area of vulnerability and mitigation assessment.

c. The provision of early warnings (i.e., the rapid sharing of information on cyber threats, vulnerabilities, and countermeasures through the issuance of cybersecurity alerts or other means).

PAWC believes that the Commission can play a vital role in the provision of early warnings. The Commission has the ability to rapidly share information regarding cyberthreats with utilities, which may mitigate or eliminate cyberthreats experienced by multiple utilities.

d. Incident response and mitigation (i.e., rapid identification of significant cybersecurity incidents and offering of assistance—e.g., personnel, services—in incident response, mitigation, or recovery).

PAWC does not see a clear role for the Commission related to incident response and mitigation.

e. Supporting Federal efforts to disrupt threat actors; and advancing cyber resiliency (i.e., developing and sharing strategies for improving overall cybersecurity resilience; facilitating use of cyber incident data to further cybersecurity research; engagement with software/equipment manufacturers on vulnerabilities and how to close them).

PAWC believes that the Commission can take a primary role in disseminating information related to cyber incident and threat data. In such a role, the Commission would support federal efforts to disrupt threat actors and advance cyber resiliency by being a resource for utilities across the Commonwealth.

f. Sharing cybersecurity threat and incident information with utility, state, and federal stakeholders for the purpose of making them aware of cybersecurity threat information that could impact their critical infrastructure or cause the potential risk to the consumer's health, safety, and/or welfare?

Similar to the above question, PAWC believes that the Commission can and should play a vital role in disseminating information related to cyber incident and threat data. Sharing information could reduce or eliminate cyber incidents experienced by utilities, and the Commission is well-positioned to effectively coordinate the dissemination of such information.

7. Should specific types of public utilities be exempt from reporting cyber incidents, and why?

PAWC believes that all utilities should report cyber incidents. However, the timing of reporting the cyber incident to the Commission should vary depending on the status of the incident. For example, if there is an active threat and the utility is working with federal law enforcement to address the threat, it would be reasonable to allow for formal notification to the Commission to be delayed.

8. Should the PUC accept incident reports submitted by a public utility to comply with another agency's regulations and if so, describe how the process could work?

PAWC believes there is value in allowing the Commission to accept incident reports submitted by a utility to comply with another agency's regulations. From an efficiency standpoint, if the information contained in the report submitted to another agency contains the same or more information than the Commission would require, there is value to being able to prepare and submit one report to meet multiple reporting requirements.

C. Questions Related to Eliminating Regulatory Duplication and Overlap

9. Given that nothing in CIRCIA or CISA's NOPR to implement CIRCIA contemplates CISA sharing any cyber incident information with the Commission, explain whether and how CIRCIA and/or CISA implementation of CIRCIA nevertheless create a potential for regulatory duplication or overlap?

For publicly traded utilities, there is considerable duplication of reporting between federal and state agencies. Such utilities would likely have to submit reports to CISA, the Securities and Exchange Commission ("SEC") and state regulators in all impacted locations.

10. If the Commission does require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks, how should the Commission eliminate regulatory duplication or overlap?

The Commission could eliminate regulatory duplication or overlap by allowing utilities to submit certifications similar to the process suggested by PAWC in response to question 2.c. above or request waivers for the use of cybersecurity programs and plans that utilize equal or stricter standards and frameworks. Additionally, the Commission could accept incident reports that were submitted by a utility to another agency if the information contained in the report is the same information, or greater information, than the Commission requires to be furnished in its incident reports.

D. Questions Related to General Topics

11. Would the elimination of the cybersecurity aspects of Chapter 101 of the PUC's regulations, as set forth in the Staff Working Proposals, impact the physical security, emergency response and/or business continuity aspects of the rule and/or Chapter 101 generally? The PUC seeks comments on the nature and extent of such foreseeable impacts and ways to address those impacts.

PAWC does not foresee the elimination of the cybersecurity aspects of Chapter 101 of the Commission's regulations, as set forth in the Staff Working Proposals, to have any impact on the physical security, emergency response and/or business continuity aspects of the rule or Chapter 101 generally.

12. Comment on how the costs and benefits associated with the Staff Working Proposals can be objectively quantified and evaluated pursuant to the Pennsylvania Regulatory Review Act, 71 P.S.§§ 745.1, et seq.

The costs and benefits of the Staff Working Proposals may be objectively quantified and evaluated by comparing the impacts of cyber incidents that were reported by utilities with a certain historical timeframe with the expected mitigation impact that the Staff Working Proposals will have on future cyber incidents.

13. Comment as to any additional considerations that you may wish to raise at this time relating to PUC oversight and regulation of public utilities as it relates to their cybersecurity fitness and/or cyber incident reporting.

PAWC does not have any additional considerations to raise at this time.

III. COMMENTS IN RESPONSE TO APPENDIX B

The Company submits the following observations in response to the Staff Working Proposals:

Proposed Section 103.1 Definitions

As previously indicated in comments above, to the extent that classes of utilities are otherwise defined in existing regulations, it may not be appropriate or practical to create new classes solely for the purpose of cybersecurity evaluations, programs, standards, and plans.

Proposed Section 103.2 Cybersecurity Evaluations and Programs

Subsection (a)(i)(B) proposes that a Class 1 utility shall maintain and adhere to an annual cybersecurity evaluation which uses the CSET. CSET is a DHS tool that is used to evaluate an organization's security posture. PAWC respectfully suggests that the tool a utility selects to conduct its cybersecurity evaluation should remain within the discretion of the utility. CISA's webpage with information concerning CSET notes, "Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations."[3] PAWC suggests that the Commission follow a similar approach in its proposed regulation that would allow utilities to select the tool that works best for each utility's unique circumstances.

[3] https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset

Proposed Section 103.3 Annual Certification

The Staff Working Proposals include a requirement of filing an annual certification that a utility adheres to the cybersecurity evaluations and programs set forth in proposed Section 103.2, but also proposes eliminating the requirement under existing 52 Pa. Code § 101.4 that a utility file a Self Certification Form. While the annual certification in proposed Section 103.3 would address some of the items that the Self Certification Form requests, it does not address all of the items (such as physical security).

Additionally, under the current regulations, the Self Certification Form is specifically acknowledged as confidential (52 Pa. Code § 101.5). The annual certification set forth in proposed Section 103.2 should similarly be acknowledged in regulations as being deemed confidential and proprietary. To the extent the Commission would wish to afford the annual certification the designation of confidential security information, the Commission should consider doing so through regulation as well.

Proposed Section 103.4 Waiver

PAWC suggests the following change to the second sentence of the proposed regulation: "A public utility must include in its petition for waiver under this section an averment that notwithstanding the requested exemption, it will maintain and comply with cybersecurity programs, plans, and standards that provide a reasonable level of cybersecurity fitness relative to its Pennsylvania assets and customers."

Proposed Section 104.2 Reporting Requirement

PAWC has concerns with subsection (a)'s requirement that a public utility shall report to the Commission any cyber incident that arises on the network of a third-party network connected to, or relied upon by, the public utility. The Company suggests that this proposed subsection be revised to include a requirement that the utility must be **aware** of the cyber incident that arises on the third-party network connected to, or relied upon, by the utility.

For subsection (a)(ii), the Company suggests that the Commission consider adding a definition for "compromise."

Subsection (a)(iii) includes a limitation that may not be intended. The "exfiltration of PI of Pennsylvania residents" may not cover all potentially impacted customers served by jurisdictional utilities providing service in Pennsylvania. For example, customers may have summer homes in Pennsylvania but reside in another state, nevertheless their PI may be exfiltrated in a cyber incident. The Company suggests revisiting the terms and perhaps modifying subsection (a)(iii) to be "exfiltration of PI of customers served by a public utility providing service in Pennsylvania."

Subsection (c) includes a proposed requirement for utilities to report to the Commission a cyber incident involving ransomware that involves one or more of the criteria in subsection (a). The reporting requirement in proposed subsection (c) directs that the utility must make its report to the Commission within 24 hours after the utility determines that a ransomware incident occurred. By contrast, proposed subsection (b) includes a reporting requirement that a public utility shall report a cyber incidents that meets one or more of the criteria in subsection (a) within 72 hours after the cyber incident occurred. The Company suggests that the reporting requirements

for subsections (b) and (c) should both be 72 hours. The Company makes this suggestion because it provides a reasonable time-frame in which the utility can detect, neutralize, and evaluate the nature of the cybersecurity incident and will help provide a more wholistic synopsis when the report is made to the Commission. Additionally, as proposed subsection (c)(i) requires the utility to include in its report "measures the utility intends to implement to ensure that it will not continue to be extorted by the ransomware actor" a 72-hour reporting timeframe seems more appropriate to enable the utility to provide to the Commission the information it seeks.

IV. CONCLUSION

PAWC thanks the Commission for this opportunity to submit comments in response to the Supplemental ANOPR following and for considering the comments contained herein.

Respectfully submitted,

Erin K. Fure (Pa. No. 312245)
Director, Corporate Counsel
Pennsylvania-American Water Company
852 Wesley Drive
Mechanicsburg, PA 17055
E-mail: erin.fure@amwater.com

Date: July 16, 2025