PENNSYLVANIA AMERICAN WATER

Teresa K. Harrold
Director, Corporate Counsel
852 Wesley Drive | Mechanicsburg, PA 17055
Phone: 717-550-1562 | Fax: 717-550-1255
teresa.harrold@amwater.com

VIA eFiling

February 8, 2023

Rosemary Chiavetta, Secretary
Commonwealth of Pennsylvania
Pennsylvania Public Utility Commission
Commonwealth Keystone Building, 2nd Floor
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:

Pennsylvania-American Water Company ("Company") is submitting the attached Comments in response to the Pennsylvania Public Utility Commission's Advance Notice of Proposed Rulemaking Order entered November 10, 2022, at the above-captioned docket.

As directed in Ordering Paragraph 9, the Company is providing these Comments in Word®-compatible format to the contact persons listed in Ordering Paragraph 8.

Should you have any questions concerning this filing, please contact me.

Sincerely,

Teresa K. Harrold

Attachment

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
ON THE ADVANCE NOTICE OF PROPOSED RULEMAKING ORDER

I. INTRODUCTION

Pennsylvania-American Water Company ("PAWC" or the "Company") submits these Comments in response to the Advance Notice of Proposed Rulemaking Order ("ANOPR") entered by the Pennsylvania Public Utility Commission ("PUC" or the "Commission") on November 10, 2022, at the above-reference docket and published in the Pennsylvania Bulletin on December 10, 2022. The ANOPR solicits comments on several policy issues related to cybersecurity, including cybersecurity self-certification and reporting requirements. Appendix A of the ANOPR identifies each of the topics on which the Commission is seeking comment. In the following section, PAWC will provide its comments regarding these topics.

II. COMMENTS

A. Sufficiency of Existing Regulations to Address Current and Future Cybersecurity Threats to Public Utilities

The Commission's cybersecurity regulations focus on two separate areas: 1) requiring all jurisdictional utilities to develop and maintain a cybersecurity plan and file an annual self-certification form that such a plan is in place,[1] and 2) requiring jurisdictional water, electric,

[1] 52 Pa. Code § 101.1, *et seq.*

and gas utilities to report "an occurrence of an unusual nature that is a physical or cyber-attack, including attempts against cyber security measures as defined in Chapter 101 that causes an interruption of service or over $50,000 in damages, or both."[2] Each of these sets of regulations were promulgated over ten years ago. More recently, the Commission adopted cybersecurity regulations for steam utilities, which differ from the reporting requirements for water, electric and gas utilities in one key respect: Steam utilities are required to report cyber security attacks "including an attempt to interfere with a steam utility's computers, software and communication networks that support, operate or otherwise interact with the steam utility's operation" whether or not they result in damages exceeding $50,000.[3]

PAWC commends the Commission's efforts to conduct a comprehensive review of its cybersecurity regulations to ensure its regulations remain current and sufficiently protective of utility infrastructure and customers. Due to the passage of time since the Commission's initial cybersecurity regulations were adopted, as well as recent federal legislation changes related to cybersecurity, the Company has a few suggestions for changes to the Commission's regulations, which are discussed in more detail below.

B. Recommended Changes to Terminology within Existing Regulations

The Commission's priorities when revising the terminology in its existing regulations should be to remove outdated terminology and promote consistency with federal cybersecurity regulation. In March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") was signed into federal law, which requires, among other things, that water utilities and other covered entities report cyber incidents to the Cybersecurity and

[2] 52 Pa. Code §§ 57.11(b)(4), 59.11(b)(5) and 65.2(b)(4).
[3] 52 Pa. Code § 61.11(b)(6).

Infrastructure Security Agency ("CISA") within 72 hours from when the incident occurred.[4] To create consistency between state and federal regulations, the Company recommends that the Commission adopt a definition for cyber incident that aligns with CISA's definition. CIRCIA requires CISA to develop and issue regulations, which may provide a more comprehensive definition for "cyber incident." To the extent CISA's rulemaking does not occur within the timeframe of the Commission's rulemaking, however, PAWC offers the following definition for "cyber incident", which is consistent with CIRCIA and other federal regulations:[5] "Cyber incident" means an occurrence that (A) actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

C. Revising Basic Security Controls Governing Cybersecurity Rulemaking

On page 10 of the Commission's ANOPR, the Commission lists the four basic security controls, which are the focus of the Commission's current cybersecurity regulations: "(1) identifying '[c]ritical functions requiring automated processing'; (2) '[a]ppropriate backup for application software and data'; (3) '[a]lternative methods for meeting critical functional responsibilities in the absence of information technology capabilities'; and (4) '[a] recognition of the critical time period for each information system before the utility could no longer continue to operate.'"[6] Based on the evolution of cybersecurity practices since the Commission's regulations were first adopted, PAWC recommends replacing (2) with the following language: "industry standard set of controls to ensure systems in a cybersecure

[4] 6 USCS § 681, *et seq.*
[5] *Id.*; *see also* 44 U.S. Code § 3552(b)(2).
[6] ANOPR at 10.

manner." The current language in (2), "appropriate backup for applicable software and data" is only one of several industry standard cybersecurity controls that are currently in place.

D. Analysis of Five Potential Regulatory Approaches to Ensure that Public Utilities Have Adequate Cybersecurity Plans in Place to Respond to Cyber Threats

The Commission lists the following five potential regulatory approaches to cybersecurity certification and requests comments on which, or which combination, of these approaches would provide the best cybersecurity protection:

1. Similar to the 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 cybersecurity measures, plans, and programs in place as a part of the management audit function.
5. Require a public utility to file a confidential copy of its cybersecurity 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.[7]

The Company agrees that approaches 1, 2, and 4 are reasonable and would help ensure that utilities are implementing industry standard cybersecurity measures. Regarding approach 3, PAWC recommends a timing modification. PAWC conducts annual penetration testing by a certified third party expert, but it only conducts a comprehensive audit of its cybersecurity program every two years. Cybersecurity technology is unlikely to change

[7] ANOPR at 12-13.

significantly on an annual basis. Therefore, PAWC recommends a biannual, as opposed to an annual, audit by a certified third-party expert.

With respect to approach 5, wherever possible, PAWC minimizes the external sharing of highly confidential information and confidential security information. Accordingly, PAWC does not support the filing of its complete cybersecurity plan at the Commission to avoid any inadvertent disclosure of such sensitive information. Instead, the Commission could modify its self-certification filing to seek more high level information regarding utilities' cybersecurity plans. A working group process with interested stakeholders would likely be the most efficiency process for developing potential changes to the self-certification filing.

E. Recommended Changes to Regulations From Actions of Other State Commissions

The Company believes that the focus of the Commission's regulations on self-certification and cyber incident reporting is reasonable and will continue to promote the adoption of robust cybersecurity procedures by utilities. To the extent the Commission is interested in reviewing other state commission approaches as part of this rulemaking, however, the Company recommends that the Commission review New Jersey's Water Quality Accountability Act, which was enacted in 2017 and includes a comprehensive cybersecurity certification and reporting program.[8]

F. Impact of Cybersecurity Changes to 52 Pa. Code § 101.3 on Physical Security, Business Continuity, and Emergency Responses Plans

Based on the information currently available in the ANOPR, changes to the Commission's cybersecurity regulations are not expected to impact the Company's physical security, business continuity, or emergency response plans. PAWC reserves the right to

[8] N.J. Stat. § 58:31-1, *et seq.*

provide further comments on this topic to the extent proposals from other parties would result in any impact to those plans.

G. Application of Self-Certification Requirements to Additional Entities

PAWC's cybersecurity plan applies to both its water and wastewater facility assets and information systems. It would be reasonable for the Commission's cybersecurity regulations to apply both to water and wastewater utilities.

H. Exemption of Entities from Self-Certification Requirements

PAWC has no comments regarding this topic at this time but reserves the right to provide further comments on this topic at future stages of this proceeding.

I. Recommendations to Improve or Streamline Self-Certification Filing or Storage Process

PAWC recommends that the Commission develop a secure portal for the filing and storage of utilities' self-certification forms. Submission of these forms via email or eFiling is not the most cybersecure method. This filing change would be increasingly important if the Commission requires more detailed information regarding utilities' cybersecurity plans to be filed in the future.

J. Recommendations to Revise Cybersecurity Reporting Criteria

PAWC supports the Commission's efforts to update its cybersecurity reporting regulations and create consistency with federal requirements. First, the Company agrees with the change the Commission made in 2017 as part of its cybersecurity regulation of steam utilities. The reporting threshold of $50,000 in damages is arbitrary and also should be eliminated from the Commission's regulations for water, gas, and electric utilities.

In addition, the Commission should strive to adopt reporting requirements that align with the federal reporting requirements within CIRCIA applicable to utilities. Consistent with

CIRCIA, utilities should be required to report all "cyber incidents" that occur to the Commission as well. PAWC recommends either (i) waiting for CISA to establish a final definition for "cyber incident" to permit the PUC to adopt an analogous definition; or (ii) adopting the definition PAWC recommends in section II(B) above.

Similarly, CIRCIA includes a 72-hour time frame for reporting cyber incidents.[9] The Company recommends that the Commission also adopt a 72-hour period for initial reports of cyber incidents. Given the potential complexity of cyber attacks, a shorter time period for reporting may not provide sufficient time for utilities to investigate cyber incidents and provide meaningful information to the Commission. It would be more efficient and useful for utility reports regarding cyber incidents to be made within 72 hours of the incidents occurring. Utilities also could be required to provide a subsequent report 30 days after such incidents to provide a more complete report to the Commission regarding the cyber incident.

K. Merging the Self-Certification and Cyber Attack Reporting Regulations

The Company supports consolidating utilities' cybersecurity self-certification and reporting requirements into separate section of the Commission's regulations. Currently, water, gas, and electric utilities' cybersecurity reporting obligations are included in the same regulation that governs accident reporting.[10] Typically, a utility's operations team is charged with responding to accident reports and a utility's information systems team is responsible for addressing cybersecurity events. Establishing a dedicated cybersecurity section of the regulations would provide better organization within the Commission's regulations and promote transparency regarding this important issue.

[9] 6 USCS § 681b.
[10] 52 Pa. Code §§ 57.11, 59.11, and 65.2.

L. Cost-Benefit Analysis of Revisions to Regulations

If the Commission adopts the proposed changes by PAWC herein, PAWC would not expect to incur significant additional costs because of the Commission's revisions to its regulations. PAWC already complies with all National Institute of Standards and Technology ("NIST") cybersecurity protocols, which PAWC considers the industry standard for cybersecurity. To the extent the final rulemaking results in new processes or procedures beyond NIST's requirements and outside the scope of the Company's recommendations herein, PAWC would need time to evaluate those changes further to determine their cost-benefit impact.

M. Eliminating State and Federal Regulatory Duplication or Overlap

As already discussed above, PAWC fully supports creating consistency between state and federal cybersecurity regulation of utilities. The adoption of consistent terminology in regulations and similar reporting timelines would help to promote such consistency.

III. CONCLUSION

PAWC is committed to maintaining a robust cybersecurity program to protect its customers, information systems, and facilities from potential cybersecurity threats. Customer safety and system reliability remain the highest priorities for the Company. The Company looks forward to continuing to work with the Commission throughout this rulemaking process to help ensure that any changes to the PUC's cybersecurity regulations are reasonable, consistent with industry standards, and in the best interest of customers.

Respectfully submitted,

Teresa Kim Harrold (Pa. No. 311082)
Director, Corporate Counsel
Pennsylvania-American Water Company
852 Wesley Drive
Mechanicsburg, PA 17055
717-550-1562
teresa.harrold@amwater.com

Dated: February 8, 2022