

Meagan Moore, Senior Attorney
Office: 412-208-6527; Mobile: 412-690-5912
Email: Meagan.moore@peoples-gas.com



Via E-file

February 8, 2023

Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street – 2nd Floor
Harrisburg, PA 17120

**RE: Advanced Notice of Proposed Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting
Docket No. L-2022-3034353**

Dear Secretary Chiavetta:

On November 10, 2022, the Pennsylvania Public Utility Commission issued an Advanced Notice of Proposed Rulemaking Order requesting review of current regulations related to cyber security self-certification and cyber-attack reporting.

Enclosed, please find the Joint Comments of both Aqua Pennsylvania, Inc. and Peoples Natural Gas Company LLC in the referenced docket.

Please contact me at meagan.moore@peoples-gas.com or (412) 208-6527 if you have any questions or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Meagan Moore", is written over a light blue horizontal line.

Meagan Moore
Counsel for Peoples Natural Gas Company LLC

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 : Docket No. L-2022-3034353
Cyber Attack Reporting :

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”) Peoples Natural Gas Company LLC (“Peoples”) (together, the “Joint Commenters”), pursuant to the Advanced Notice of Proposed Rulemaking Order (“ANOPR”) published in the Pennsylvania Bulletin on December 10, 2022, to file these comments with the Pennsylvania Public Utility Commission (“PUC” or the “Commission”). The ANOPR proposes to “review its current regulations relating to cybersecurity.” These regulations fall into two groups: (1) cyber-attack reporting regulations¹ and (2) self-certification² regulations (collectively, “existing regulations”).

I. INTRODUCTION

Aqua and Peoples are Class A water and natural gas utilities operating under Commission issued certificates of public convenience. Aqua serves approximately 448,000 water customers and, through its subsidiary Aqua Pennsylvania Wastewater, Inc., 60,000 wastewater customers in various counties throughout Pennsylvania. Peoples serves approximately 700,000 natural gas customers in various counties throughout Pennsylvania. Joint Commenters commend the

¹ 52 Pa. Code §§ 57.11 (relating to accidents) for electric 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.

² 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.

Commission for its continued initiatives to ensure regulations are updated to address the ever-changing issues in cyber security. Joint Commenters are supportive of updating cybersecurity measures to better reflect the current cybersecurity landscape. It is with this background that the Joint Commenters provide the following suggestions for the Commission's consideration regarding cybersecurity regulations.

II. BACKGROUND

The PUC's self-certification regulations were first promulgated in 2005 to require "all jurisdictional utilities to develop and maintain written physical, cyber security, emergency response and business continuity plans to protect the Commonwealth's infrastructure and ensure safe, continuous and reliable utility service."³ The PUC promulgated cyber-attack reporting regulations for electric, gas and water public utilities in 2011, broadening the scope of the previously existing cyber-attack reporting regulations to include "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."⁴ Section 101.2 defines "cyber security" as "[t]he measures designed to protect computers, software and communications networks that support, operate or otherwise interact with the company's operations." Joint Commenters acknowledge the statutory bases for the cyber-attack reporting regulations and the self-certification regulations within Sections 501, 504, 505, 506, and 1501 of the Public Utility Code, 66 Pa.C.S. §§ 501, 504, 505, 506 and 1501.⁵

The ANOPR specifically asked commenters to address certain questions. These questions are considered in each section as they are introduced in the ANOPR. The ANOPR asks whether

³ Revised Final Rulemaking Order, Rulemaking re Public Utility Security Planning and Readiness, Pa. PUC Docket No. L-00040166 (entered Mar. 10, 2005) at 1, 35 Pa.B. 24 (June 11, 2005) (Chapter 101 Order).

⁴ See 52 Pa. Code §§ 57.11(b)(4), 59.11(b)(5) and 65.2(b)(4).

⁵ Chapter 101 Order at 29; Outage Response Order ([Docket No. I-2011-2271989](#)) at 36.

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.⁶

Joint Commenters are overall supportive of cybersecurity requirements ensuring protection of sensitive assets. Existing regulations have been appropriate and ensure public utility fitness while allowing for discretion to create appropriate cybersecurity plans for each unique utility. Joint Commenters recommend that revised regulations are consistent with federal requirements, are non-duplicative, and do not require a specific framework given the scope of regulated utilities a potential rulemaking will impact. As an example, while many utilities align to the National Institute of Standards and Technology Cybersecurity Framework (“NIST CSF”), other utilities may have specific requirements that leads to a more prescriptive framework such as those in scope for North American Electric Reliability Corporation Critical Infrastructure Protection (“NERC CIP”) in the electric sector. Joint Commenters assert that the focus of proposed regulations should be on ensuring implementation of appropriate controls that provide effective risk mitigation, rather than a prescribed framework. If a specific framework will be required, Joint Commenters support the NIST CSF.

III. DISCUSSION

A. Updating Terms and Concepts

Overall, Joint Commenters recommend terms and concepts that are consistent with existing cybersecurity requirements and are uniform across Pennsylvania state agencies, with a focus on specific actions within the purview of the PUC.

For incident and cyber-attack reporting requirements, the language must be clear on defining the right type of security events and conditions for reporting. Utility security leaders see

⁶ ANOPR at 2.

security events continuously every day, and the vast majority are of little value from a reporting perspective as the controls currently implemented effectively address these events. Joint Commenters believe it is important for proposed terms and concepts to adequately define the conditions and specific scenarios for reporting material and impactful or declared incidents and identify how this information will be used by the PUC.

B. Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities

The ANOPR outlines five potential regulatory approaches based on the Commission's review of federal practices.

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 annual 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.⁷

⁷ ANOPR at pp. 12-13.

Joint Commenters are generally supportive of Options 1, 2, and 4. Joint Commenters do not believe a requirement to obtain third-party auditing, certification, or attestation should be implemented due to the costly operational burden. It would be overly burdensome and inconsistent if each state had different requirements for an independent cybersecurity audit and third-party certification. Further, regarding Option 4, the Joint Commenters submit that the Commission's audit staff already interviews and reviews utilities' cybersecurity programs through their management audit process. Overall, Joint Commenters recommend that the approach requires self-certification ensuring appropriate and effective security controls are in place, along with regularly scheduled program review discussions and management audit reviews.

Joint Commenters are concerned about any potential requirement for utilities to submit highly sensitive risk and vulnerability data directly to the PUC. The Joint Commenters believe that the Commission's existing process of reviewing cybersecurity information at on-site meetings through the Commission's audit staff, where no sensitive data is transmitted or taken off-site is sufficient. Other states' methods generally focus on understanding our practices, but do not directly collect highly sensitive information from the organization. In New Jersey, under the Water Quality Accountability Act ("WQAA"), which was expanded with additional requirements in 2022, annual cyber risk profiles are to be completed. These profiles include assets for information technology ("IT") and operations technology ("OT") in New Jersey covering a range of the implemented controls and processes. Secondly, New Jersey Utilities participate in a monthly working group hosted by the New Jersey Board of Public Utilities ("NJ BPU") for cybersecurity leaders across the regulated utilities in New Jersey. Finally, utilities register official contacts for security personnel with the New Jersey Communications & Cybersecurity Integration Cell

(“NJCCIC”). While a cyber controls and risk management questionnaire is submitted, a specific framework is not mandated.

Additionally, it is crucial to know exactly how this type of data will be used, and how the PUC will protect this sensitive data if required to collect it. At the federal level, there are protections within Title 6 CFR Part 29 Protected Critical Infrastructure Information to exclude sensitive critical infrastructure information from Freedom of Information Act (“FOIA”) requests. Under state and local laws this information is similarly protected and excluded from use in regulatory proceedings and civil action. Again, the Joint Commenters urge the Commission not to adopt any regulation that requires the submission of sensitive cybersecurity information to the Commission; however, if this information is to be collected it is crucial to understand how the PUC will ensure that there is no unauthorized disclosure or access to the utilities’ sensitive information.

The ANOPR asks whether changes to the cybersecurity portion of 52 Pa. Code § 101.3 would impact the rules at Chapter 101.⁸ Joint Commenters prefer to provide specific comment upon a proposed rule but believe there should be clarity between the requirement to report cybersecurity and physical security incidents. There is a potential impact to cybersecurity, physical security, and business continuity with any changes to cybersecurity requirements.

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

Joint Commenters do not recommend any changes at this time and are agreeable to continuing a policy of self-certification that allows the PUC to hold a utility responsible for reporting that it has a cybersecurity program, that it has been reviewed and tested annually, and to

⁸ ANOPR at 13.

provide a vehicle for addressing utility deficiencies in a manner that does not increase regulatory burdens and costs.

D. Updating Cyber Attack Reporting Regulations

As previously stated, any updated regulations must be clear on defining the right type of security events and conditions for reporting. The proposed terms and concepts must adequately define the conditions and specific scenarios for reporting material and impactful or declared incidents and identify how this information will be used by the PUC. Any requirement for the immediate reporting of declared incidents should clearly identify what constitutes an incident as ‘immediate’. Limiting the scope of reportable incidents to those with a material impact, rather than only a monetary impact, is crucial, but the level of impact to trigger such reporting to the PUC needs to be clearly defined and measurable.

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

Joint Commenters are not opposed to the merging of cyber-attack requirements but recommend that the requirements remain broad enough for utility applicability while clearly laying out procedure and compliance.

F. Cost Benefit Analysis

Joint Commenters do not believe there is any discernable benefit to updating cybersecurity reporting requirements at this time and will further comment with regards to cost benefit analysis upon the issuance of a proposed rule.

G. Eliminating Regulatory Duplication and Overlap

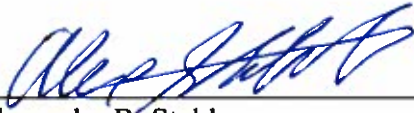
Avoiding unnecessary regulatory duplication and overlap is of great benefit to all regulated entities and prevents unnecessary operational burden. As stated above, there are various existing requirements at the state and federal level that currently provide an adequate level of reporting.

Additionally, the new federal Cyber Incident Reporting Critical Infrastructure Act (“CIRCI”) was adopted in March 2022. Final rules are still in development, and Joint Commenters feel that any PUC proposed rules should attempt to remain consistent with these impending federal requirements.

IV. CONCLUSION

Aqua and Peoples appreciate the opportunity to comment on the Advanced Notice of Proposed Rulemaking and ask that the Commission consider their comments. Aqua and Peoples look forward to continuing to work with the Commission on these issues. Please direct any questions with regard to these comments to the undersigned.

Respectfully Submitted,



Alexander R. Stahl
Regulatory 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