



**UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
REGION III
Four Penn Center
1600 John F Kennedy Blvd
Philadelphia, Pennsylvania 19103-2852**

January 30, 2023

Gladys Brown Dutrieuille, Chairman
Pennsylvania Public Utility Commission
Commonwealth Keystone Building, 2nd Floor
400 North Street
Harrisburg, PA 17120

Filed electronically at: www.puc.pa.gov/filing-resources/efiling/

Dear Chairman Dutrieuille:

On December 10, 2022, the Pennsylvania Public Utility Commission (PUC) published an Advanced Notice of Proposed Rulemaking (ANOPR) in the *Pennsylvania Bulletin* pertaining to cybersecurity, Docket No. L-2022-3034353. Specifically, the PUC seeks comments from interested stakeholders, including members of the regulated industry, statutory advocates, the public, and any other interested parties about whether the existing regulations are sufficient or if they need to be revised to ensure that they address public utility fitness in the current and anticipated future cybersecurity threat landscapes.

The Environmental Protection Agency (EPA) is designated as the Sector Risk Management Agency for the Water and Wastewater Systems Sector and offers the following comments and recommendations for the PUC's consideration. Comments apply to the water and wastewater sector. Comments are organized by topics of PUC interest as noted in the ANOPR.

Updating Terms and Concepts

PUC should consider updating its definition of "Cybersecurity" to also include operational technology (OT). This definition should be updated to align more closely with the National Institute of Standards and Technology (NIST), U.S. Department of Commerce definition.

The PUC's definition of a cybersecurity plan should be updated to more closely align with the terms outlined in this section of the regulation. Using NIST's definitions of these common cyber terms will better reflect the current cybersecurity landscape, and Federal and industry standards.

Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities Improving the Self-Certification Form (SCF) Process

A key concern with the self-certification approach is that the small and medium water utilities may lack the resources to develop and implement an adequate plan and may never learn how to improve their cybersecurity if there isn't any PUC review and feedback provided on their

plans. These plans need to be reviewed and tested annually. However, if utilities have to self-certify the concern is that many utilities may see this as another ‘check in the box exercise’ and not prioritize this process to address real world concerns.

Requiring a "third-party expert certification" is somewhat ambiguous. It is necessary to define what the PUC considers the credentials of an expert third-party and the details of what they are certifying. There are no such experts defined by others that EPA is aware of. Additionally, has the PUC considered who would be paying for these third-party assessments and certification - the state or the utility?

The ANOPR lists five potential regulatory approaches for comment. The last two approaches would be most effective. As noted above, this enables the PUC to review and provide feedback on each plan; therefore, the utility can learn where deficiencies exist in their plan and how to improve.

It should be noted that EPA will be issuing a memo in FY’23 which will provide our long-term goal of state drinking water programs incorporating cybersecurity into the on-site sanitary surveys conducted at water utilities. This program is implemented by the Bureau of Safe Drinking Water, Pennsylvania Department of Environmental Protection (PA DEP). Close coordination with PADEP and the PUC on similar cybersecurity measures will be necessary to avoid unnecessary duplication of efforts by the utilities.

What would be the frequency of these PUC on-site audits of utility security measures, plans and programs? Yearly, every two years, or another frequency?

Updating Cyber Attack Reporting Regulations

It is recommended that the PUC expand the current thresholds for cyber reporting. For example, similar to the incident in Oldsmar, FL if a cyber threat actor is able to gain access to the network to alter chemical levels but the change is prevented by operators there won’t be an interruption to service nor any financial damages; therefore, the incident will not meet the requirement to be reported to the PUC, as currently stated. It would be in the state's best interest to know about incidents such as this in a timely manner.

Merging the Self-Certification Form (SCF) and Cyber Attack Reporting Regulation

This process could be streamlined by the creation of a secure online portal that utilities can access to upload their SCF documents and both PUC and the utility can track the processing of the SCF submission.

For incidents affecting drinking water and wastewater utilities it is recommended that the population served/impacted by a cyber incident would be a good reporting threshold.

Eliminating Regulatory Duplication and Overlap

Considering that the implementation and reporting aspects of the Federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) are still under development, it is recommended that the PUC leadership contact the Cybersecurity and Infrastructure Security

Agency (CISA) to learn their thoughts and approach on CIRCIA development. The PUC may be able to leverage some of the same strategies for improving the Self-Certification Regulations and create consistencies now without the need for possible future rule changes. CIRCIA will also address ransomware incidents.

Other Matters

As noted above, EPA is considering taking action(s) that would impact implementation of sanitary surveys by the drinking water program in the Bureau of Safe Drinking Water, PA DEP. Plans are in the development stages and we will ensure that the PA PUC receives information regarding any action EPA undertakes.

These comments are provided by EPA's Water Infrastructure and Cyber Resilience Division and Region 3's Water Division. Please direct any questions to Patti Kay Wisniewski at Wisniewski.patti-kay@epa.gov.

Sincerely,

Patti Kay Wisniewski
Drinking Water Security/Preparedness Coordinator
Drinking Water Section (3WD21)