Hawke McKeon & Sniscak LLP
ATTORNEYS AT LAW

Thomas J. Sniscak
(717) 236-1300 x224
tjsniscak@hmslegal.com

Whitney E. Snyder
(717) 236-1300 x260
wesnyder@hmslegal.com

Phillip D. Demanchick Jr.
(717) 236-1300 x225
pddemanchick@hmslegal.com

100 North Tenth Street, Harrisburg, PA 17101 Phone: 717.236.1300 Fax: 717.236.4841 www.hmslegal.com

February 8, 2023

Via Electronic Filing

Rosemary Chiavetta, Secretary
Secretary's Bureau
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, Second Floor
Harrisburg, PA 17120

RE: Advance Notice of Proposed Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Accident Reporting; Docket No. L-2022-3034353; **JOINT COMMENTS OF COMMUNITY UTILITIES OF PENNSYLVANIA INC. AND COLUMBIA WATER COMPANY**

Dear Secretary Chiavetta,

Enclosed for filing are the Joint Comments of Community Utilities of Pennsylvania Inc., and Columbia Water Company.

Thank you for your attention to this matter. If you have any questions, please feel free to contact me at (717) 236-1300.

Respectfully submitted,

/s/ Phillip D. Demanchick Jr.

Thomas J. Sniscak
Whitney E. Snyder
Phillip D. Demanchick Jr.

Counsel for
Community Utilities of Pennsylvania Inc., and Columbia Water Company

PDD/das
Enclosure
cc: Colin Scott, Law Bureau (colinscott@pa.gov)
Chris Van de Verg, Law Bureau (cvandeverg@pa.gov)
Daniel Searfoorce, BTUS (dsearfoorc@pa.gov)
Michael Holko, OCCO (miholko@pa.gov)
Karen Thorne, Law Bureau (kathorne@pa.gov)

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 COMMUNITY UTILITIES OF PENNSYLVANIA, INC. AND COLUMBIA WATER COMPANY

Thomas J. Sniscak, Esq. (PA ID No. 33891)
Whitney E. Snyder, Esq. (PA ID No. 316625)
Phillip D. Demanchick Jr., Esq. (PA ID No. 324761)
Hawke McKeon & Sniscak LLP
100 North Tenth Street
Harrisburg, PA 17101
Tel: (717) 236-1300
tjsniscak@hmslegal.com
wesnyder@hmslegal.com
pddemanchick@hmslegal.com

Counsel for Community Utilities of Pennsylvania, Inc., and Columbia Water Company

Dated: February 8, 2023

I. INTRODUCTION

On November 10, 2022, the Pennsylvania Public Utility Commission ("Commission" or "PUC") entered an Advance Notice of Proposed Rulemaking Order ("ANOPR") seeking to review its current regulations relating to cybersecurity, including (1) the Cyber Attack Reporting Regulations[1] and (2) the Cybersecurity Self-Certification Regulations[2] (collectively, "Cybersecurity Regulations"). In conjunction with the ANOPR, the Commission issued Appendix A containing a list of 15 discrete topics for consideration and comment by interested stakeholders. The ANOPR was published in the Pennsylvania Bulletin on December 10, 2022, with Comments due 60 days after publication.

Community Utilities of Pennsylvania, Inc. ("CUPA") and Columbia Water Company ("CWC") provide the following Joint Comments, which are summarized here and discussed in more detail in Section II.

- The Commission must seek to appropriately balance safety, security, cost, and flexibility when regulating utility cybersecurity practices. The Commission should not adopt onerous or one-size-fits-all requirements for public utilities. Otherwise, it could make compliance unreasonably difficult for smaller utilities, create time consuming requirements that may lag behind emerging cyber threats, and impede cooperation between the Commission and utilities to address future cybersecurity concerns.

- The current Cybersecurity Self-Certification Regulations provide the necessary discretion to utilities to establish and develop cybersecurity practices best suited for the needs of their organization and the risks it faces.

[1] 52 Pa. Code §§ 57.11 (relating to accidents for electricity 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) (collectively, "Cyber Attack Reporting Regulations").

[2] 52 Pa. Code §§ 101.1, *et seq*. (relating to public utility preparedness through self-certification for jurisdictional utilities); *see also* 52 Pa. Code § 61.45 (relating to security planning and emergency contact list for steam utilities) (collectively, "Cybersecurity Self-Certification Regulations").

- Should the Commission decide to create new requirements, it should only modify its existing framework to address any desired outcomes to allow a utility to iteratively address the Commission's concerns in a measured way.

- Should the Commission substantially revise its Cybersecurity Regulations, the Commission should: (1) include utility stakeholders to help steer and guide the process; and (2) exempt smaller utilities that do not have the financial or technical resources of larger utilities.

- Compliance with a federal or industry standard is not appropriate given that: (1) different utility sectors are subject to unique risks and requirements; and (2) cybersecurity standards are generally meant to be flexible and are not meant to be applied prescriptively or as a one-size-fits all solution.

- CUPA and CWC strongly urge that the Commission establish a phase-in or delayed compliance period of at least one year, if not more, to provide utilities the necessary time to reach compliance with any new standards that are adopted, with additional phase-ins for smaller utilities if required to comply.

- Any costs required to meet new or additional cybersecurity requirements must be subject to cost recovery in a utility's base rates.

II. COMMENTS

A. Introduction

While CUPA and CWC appreciate the Commission's efforts to review its current Cybersecurity Regulations, CUPA and CWC urge the Commission to exercise caution if it intends to create new cybersecurity standards that apply to jurisdictional utilities. Ultimately, with cybersecurity regulation, the Commission must seek to appropriately balance safety, security, cost, and flexibility. In other words, it is incumbent upon the Commission not to adopt onerous or one-size-fits-all requirements for jurisdictional public utilities. Otherwise, it could make compliance unreasonably difficult for smaller utilities, create time consuming requirements that may lag behind emerging cyber threats, impede cooperation between the Commission and utilities to address future cybersecurity concerns, and result in increased rates for customers. Rather, voluntary or broad goal-based standards, such as the National Institute of Standards and

Technology's ("NIST") Cybersecurity Framework, provides the necessary discretion to organizations to identify discrete goals for improving their cybersecurity practices that best suits each utility and addresses the risks involved.[3]

For this reason, CUPA and CWC submit that the Commission's current Cybersecurity Self-Certification Regulations provide the necessary discretion to its utilities to establish and develop cybersecurity practices best suited for the needs of their organization and the risks it faces. Indeed, the Commission's current requirements are beneficial in several ways because (1) it sufficiently identifies cognizable goals that each utility should achieve as part of its cybersecurity plan[4], (2) requires annual updates, testing, and self-certification for compliance[5], (3) allows the Commission to review a public utility's cybersecurity plan or inspect utility facilities as necessary[6], and (4) provides appropriate deference to cybersecurity plans created under the directive of another state or federal entity that otherwise meets the requirements of 52 Pa. Code § 101.3.[7]

Ultimately, CUPA and CWC take cybersecurity concerns very seriously and have taken efforts to develop its cybersecurity practices to identify and prevent threats to its informational and operational systems. CUPA and CWC are committed to addressing cybersecurity threats

---

[3] Through the Cybersecurity Enhancement Act of 2014 ("CEA"), NIST's role was updated to include identifying "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, at v (Version 1.1 2018), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[4] A cybersecurity plan requires, at a minimum, (i) critical functions requiring automated processing, (ii) appropriate backup for application software and data, which may include having a separate distinct storage media for data or a different physical location for application software, (iii) alternative methods for meeting critical functional responsibilities in the absence of information technology capabilities, and (iv) a recognition of the critical time period for each information system before the utility could no longer continue to operate. 52 Pa. Code § 101.3(a)(2). Such a plan shall also include defined roles and responsibilities by individual or job function. 52 Pa. Code § 101.3(e).

[5] 52 Pa. Code § 101.3(b)-(d).

[6] 52 Pa. Code § 101.6(b)-(c).

[7] 52 Pa. Code § 101.6(d).

consistent with their responsibility under the Public Utility Code to furnish and maintain adequate, efficient, safe, and reasonable service and facilities. 66 Pa. C.S. § 1501. To otherwise now impose significant or burdensome Commission oversight that does not afford the utility flexibility in its approach to cybersecurity can lead to outdated or misguided practices that either lag behind or improperly prioritize emerging threats to utility assets.

Notwithstanding, should the Commission decide to move forward with expanding its Cybersecurity Regulations, CUPA and CWC recommend that the Commission simply modify its existing regulatory framework to address any outcomes or results-oriented goals that the Commission desires to see added to a utility's cybersecurity plan. This would ensure continued stability in a utility's current cybersecurity practices, allow a utility to iteratively address the Commission's concerns in a measured way, and maintain the critical exemption that allows a utility to satisfy the Commission's Cybersecurity Self-Certification Regulations if it is subject to a cybersecurity plan under the directive of another state or federal entity. This exemption is particularly important for utilities that are owned and operated by holding companies that maintain utility operations in several states and must coordinate consistent cybersecurity practices across their organizational affiliates.

Lastly, if the Commission decides to create new cybersecurity requirements, which CUPA and CWC do not believe is necessary, it is imperative that utility stakeholders are included and help steer the process for establishing industry-wide cybersecurity standards in Pennsylvania. Doing so, ensures that any new or modified Pennsylvania-specific cybersecurity standards are consistent with other state and federal standards, establishes standards appropriately adapted to the regulated utilities, and will encourage cooperation between the Commission and utilities.

B. Updating Terms and Concepts

CUPA and CWC are not opposed to the Commission updating its terms and concepts to be consistent with other federal and industry standards where appropriate. To the extent that new requirements are established, the Commission should ensure that it carefully defines terms so as not to be inconsistent with generally accepted standards, such as NIST's Cybersecurity Framework.

C. Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities

The Commission proposes several discrete approaches to revising its cybersecurity regulations that it is considering as part of this ANOPR. This includes the following approaches:

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.

The Commission has asked for comments as to the merits and weaknesses of each approach, whether such changes would interfere with the other requirements set forth in 52 Pa. Code § 101.3, whether other jurisdictional utilities not currently subject to these requirements should be, and whether certain utilities should be wholly or partially exempt from these requirements.

CUPA and CWC submit that the current approach is adequate to ensure that regulated utilities are updating and certifying the existence of cybersecurity plans that comply with 52 Pa. Code § 101.3. To the extent there are any additional risks or results that the Commission seeks to address as part of a utility's cybersecurity plan, it could modify the existing framework to allow utilities to iteratively address those risks as part of its current cybersecurity plan.

CUPA and CWC do not believe it is appropriate, however, to compel compliance with an existing federal or industry standard. For one, each utility group has different risks and needs that it must address as part of its cybersecurity plan, which makes it difficult to mandate one standard for all utility groups. For example, the North American Electric Reliability Corporation's ("NERC") Critical Infrastructure Protection ("CIP") Standards are cybersecurity standards specific to electric utilities that operate equipment on the bulk electric system. Thus, Pennsylvania's electric utilities may operate cybersecurity plans that adhere to NERC's CIP to remain consistent with organizational affiliates and satisfy applicable federal standards. These standards do not apply to other utility industries.

Furthermore, other standards, such as NIST's Cybersecurity Framework are not meant to be prescriptive requirements-based standards, but are rather general, voluntary standards that seek to guide organizations to better understand their current cybersecurity capabilities and improve their cyber-risk profiles over time. Enforcing compliance with NIST's Cybersecurity Framework is not only counter-intuitive, but it also will be difficult to establish a uniform standard applied to

all jurisdictional utilities. More specifically, NIST's Cybersecurity framework is a collection of functions, sub-categories of each function, risk profile types, and implementation tiers that are designed to allow organizations —regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving security and resilience. With this high degree of flexibility and specification inherent in NIST's Cybersecurity Framework, it will be difficult for the Commission to craft a generally applicable standard to guide utility conduct, particularly for those smaller utilities that do not have the resources of a larger utility to implement any prescriptive standards set by the Commission.

Third-party certification also poses additional concerns as it would create significant costs passed on to ratepayers, establish a time-consuming process requiring selection of a third party to perform and complete the auditing process, and potentially result in inconsistent recommendations between utilities given the high-degree of flexibility inherent in certain cybersecurity standards. Certainly, the costs and burdens associated with third-party certification would weigh heavily on smaller utilities, such as CUPA, CWC, and their ratepayers. Ultimately, CUPA and CWC submit that the time and expense involved would heavily outweigh the benefits, particularly when CUPA and CWC already work to establish cybersecurity protocols to protect its informational and operational technology systems.

As to approaches four and five, CUPA and CWC note that the Commission can presently review a utility's cybersecurity plan pursuant to 52 Pa. Code § 101.6(b).[8] However, CUPA and CWC do have concerns if the Commission implements a requirement that a public utility must file a confidential copy of its cybersecurity plan with the Commission for comment and review. For

[8] 52 Pa. Code § 101.6(b) ("The Commission may review a utility's cyber security plan, physical security plan, emergency response plan and business continuity plan under 66 Pa. C.S. § § 504—506 (relating to reports by public utility; duty to furnish information to commission; and inspection of facilities and records).").

one, CUPA and CWC believe that it is best to limit access to these documents as much as possible to prevent bad actors from obtaining them. Thus, CUPA and CWC do not believe filing a copy with the Commission, even if marked confidential, should be required by each public utility. If, however, the Commission desires to do so, a cybersecurity plan must be designated as Confidential Security Information ("CSI") subject to the protections of the Public Utility Confidential Security Information Disclosure Protection Act.[9] Additionally, for the same reasons as identified above, allowing for Commission comment and review of a public utility's cybersecurity plan would not be appropriate given that each utility must craft a plan that is specific to their organization and it would lead to inconsistent Commission enforcement between utilities based on broad, flexible standards that should not be applied prescriptively. For these reasons, CUPA and CWC continue to submit that the current process is sufficient.

Lastly, while CUPA and CWC do not believe new cybersecurity standards should be implemented, should the Commission decide otherwise, CUPA and CWC strongly urge that the Commission allow exemptions for smaller utilities that do not have the financial or technical resources of larger utilities. The Commission's goal should be to foster cooperation and the protection of critical utility assets, not to penalize smaller utilities for their inability to maintain the same risk profiles as their larger counterparts.

[9] CUPA and CWC submit the Commission should clarify in any rulemaking requiring submission of cyber security plans or related documents that the Public Utility Confidential Security Information Disclosure Protection Act applies to those documents. *See* 35 P.S. §§ 2141.1, *et seq.* The Public Utility Confidential Security Information Disclosure Protection Act states that CSI should encompass both (1) "portions of emergency response plans that are submitted to…the Pennsylvania Public Utility Commission…dealing with response procedures or plans prepared to prevent or respond to emergency situations…the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures or specific security procedures," and (2) "[a] security plan, security procedure or risk assessment prepared specifically for the purpose of preventing or for protection against sabotage or criminal or terrorist acts." 35 P.S. § 2141.2.

D. Updating Cyber Attack Reporting Regulations

The Commission seeks comment on potential ways to revise the reporting criteria in its Cyber Attack Reporting Regulations, including the potential addition of new requirements for reporting incidents involving information technology. ANOPR at 17. The Commission also seeks comment with respect to the continuing efficacy of the $50,000 reporting threshold. ANOPR at 17.

As the Commission noted in its ANOPR, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") was signed into law and directs the Cybersecurity and Infrastructure Security Agency ("CISA") to develop regulations requiring covered entities to submit reports detailing covered cyber incidents and ransom payments within 72 hours from the time the entity reasonably believes the incident occurred.[10] It is likely that public utilities will be considered covered entities subject to these reporting requirements.[11] However, the CISA rulemaking process is ongoing and in its infancy with CISA expected to publish a Notice of Proposed Rulemaking by March 2024. As part of this process, CISA's proposed requirements will be subject to public comment and requires CISA to consult with various entities throughout the rulemaking process, including Sector Risk Management Agencies ("SRMA"), the Department of Justice ("DOJ"), other appropriate federal agencies, and a soon-to-be formed U.S. Department of Homeland Security ("DHS")-chaired Cyber Incident Reporting Council. For these reasons, it may

---

[10] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Div. Y, 136 Stat. 49, 1038-1059 (2022) (codified at 6 U.S.C. §§ 681, et seq.) (Cyber Incident Reporting for Critical Infrastructure Act of 2022).

[11] CIRCIA defines a 'covered entity' as an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b). 6 U.S.C. § 681. Presidential Policy Directive 21 defines critical infrastructure sectors to include, among other things, energy and water and wastewater systems. OFFICE OF THE PRESS SECRETARY, THE WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE 21, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

be appropriate to wait until CISA finalizes its rulemaking to avoid being inconsistent with federal standards and to create synergies with new federal reporting requirements regarding cyber incidents and ransom payments.

As to the continued efficacy of the $50,000 reporting threshold, CUPA and CWC are not opposed to the Commission clarifying how the damages attributed to a cyberattack should be calculated, what costs should be considered damages, and when the calculation should be performed. Indeed, guidance can be helpful for determining compliance with the Commission's requirements. However, CUPA and CWC do not believe the reporting threshold as it relates to cyberattacks should be reduced or eliminated altogether. To otherwise reduce or eliminate this threshold could create burdensome reporting requirements and result in overreporting from jurisdictional utilities, making it difficult to focus on the most important and critical cyberattacks should they arise.[12] Moreover, if a cyber incident resulted in the interruption of service, the utility is still obligated to report the incident regardless of whether the damage threshold is met. *See, e.g.*, 52 Pa. Code § 65.2. This ensures that any cyber incidents that affect critical infrastructure resulting in interruption of service or loss of service to a customer are brought to the Commission's attention in a timely manner.

E. Eliminating Regulatory Duplication and Overlap

The PUC seeks comment on the potential for conflict, overlap, redundancy, or other bases warranting review in the interplay between the PUC's cybersecurity regulations (and revisions

[12] As justification for the $50,000 threshold when it was initially implemented, the Commission stated, "[t]he Commission agrees that cyber-attacks that result in an interruption should be reported to the Commission but also contends that those attacks that result in over $50,000 in damages should also be reported because this is a large enough threshold that it will not burden utilities with reporting everyday minor incidences. If we required them to report every cyber attack, this would require a significant amount of reporting since this happens every day. We changed this to make the requirement threshold $50,000 in damages. This threshold is significant damages so that every daily incident will not be reported. This is also consistent with the federal regulations." *Utilities' Service Outage Response and Restoration Practices*, 42 Pa. B. 9, 15 (Jan. 7, 2012).

thereto) and federal initiatives, including but not limited to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). See ANOPR at 21.

The Commission should be aware that at the time of these Joint Comments, the NIST Cybersecurity Framework is currently being updated and subject to public review and comment, with feedback requested by March 3, 2023 ("Cybersecurity Framework 2.0").[13] As part of Cybersecurity Framework 2.0, NIST is proposing to add a new 'govern' function to emphasize cybersecurity risk management governance outcomes, such as determination of priorities and risk tolerances of the organization, customers, and larger society; assessment of cybersecurity risks and impacts; establishment of cybersecurity policies and procedures; and understanding of cybersecurity roles and responsibilities.[14] NIST is also looking to provide additional guidance regarding how to measure and assess an organization's use of the Cybersecurity Framework.[15] Final publication of the Cybersecurity Framework 2.0 is expected in Winter 2024. The Commission may want to follow these developments as it considers whether new cybersecurity requirements are necessary.

Moreover, as stated by NIST, the Cybersecurity Framework is intended to be a living document that is refined and improved over time.[16] Similarly, NERC continually updates its CIP Standards over time to address new or emerging needs. For this reason, the Commission should be careful not to develop or create standards that risk becoming stale or inconsistent with other industry standards as a result. For example, as discussed above, the Commission should wait until

---

13 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST CYBERSECURITY FRAMEWORK 2.0 CONCEPT PAPER: POTENTIAL SIGNIFICANT UPDATES TO THE CYBERSECURITY FRAMEWORK (2023), available at https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf.

14 *Id*., at 10.

15 *Id*., at 12.

16 *Id*., at 3.

CISA develops its new reporting requirements pursuant to CIRCIA before it considers changing its existing Cyber Attack Reporting Regulations. Accordingly, CUPA and CWC submit that creating prescriptive standards that may become outdated shortly after publication is not in the public interest.

F. Other Matters

Should the Commission decide to create new or modified Cybersecurity Regulations, CUPA and CWC strongly urge that the Commission establish a phase-in or delayed compliance period to provide utilities the necessary time to reach compliance with the new standards. Phasing-in compliance with these regulations is appropriate given that new Cybersecurity Regulations could require significant modification to existing utility cybersecurity plans. CUPA and CWC submit that the Commission should consider delaying compliance by at least one year from publication of the final rulemaking in the Pennsylvania Bulletin, if not longer depending on the extent of the new requirements. Moreover, the Commission should provide additional time for smaller utilities to comply should it decide to apply these new requirements to smaller regulated utilities.

Lastly, any costs required to meet new or additional cybersecurity requirements must be subject to cost recovery in a utility's base rates. Utilities are entitled to recover its reasonable and prudent expenses. *Pennsylvania Power & Light Co. v. Pa. Pub. Util. Comm'n*, 311 A.2d 151, 155-56 (Pa. Cmwlth. 1973). This should be no exception.

III. CONCLUSION

Community Utilities of Pennsylvania, Inc. and Columbia Water Company appreciate the opportunity to submit its Joint Comments regarding the Commission's Advanced Notice of Proposed Rulemaking. CUPA and CWC encourage the Commission to maintain its existing Cybersecurity Regulations, which provide each utility organization with the necessary managerial discretion to establish, maintain, and modify a cybersecurity plan that best fits the risk each utility faces. Any onerous, or one-size-fits all requirements could make compliance unreasonably difficult for smaller utilities, create time consuming requirements that may lag behind emerging cyber threats, and impede cooperation between the Commission and utilities to address future cybersecurity concerns. To the extent that the Commission desires to create any new or additional standards, it should do so in a measured, iterative manner, in close cooperation with its jurisdictional utilities. There should also be some recognition from the Commission that any additional costs incurred as part of new cybersecurity standards must be subject to cost recovery in a utility's base rates.

Respectfully Submitted,

/s/Phillip D. Demanchick Jr.
Thomas J. Sniscak, Esq. (PA ID No. 33891)
Whitney E. Snyder, Esq. (PA ID No. 316625)
Phillip D. Demanchick Jr., Esq. (PA ID No. 324761)
Hawke McKeon & Sniscak LLP
100 North Tenth Street
Harrisburg, PA 17101
Tel: (717) 236-1300
tjsniscak@hmslegal.com
wesnyder@hmslegal.com
pddemanchick@hmslegal.com

Counsel for Community Utilities of Pa., Inc., and Columbia Water Company

Dated: February 8, 2023