Emily Farah
Assistant General Counsel
Legal Department

121 Champion Way, Ste. 100
Canonsburg, PA 15317
(724) 416-6321
efarah@nisource.com

July 15, 2025

VIA ELECTRONIC FILING

Matthew L. Homsher, Secretary
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 Homsher:

Enclosed for filing please find Columbia Gas of Pennsylvania, Inc.'s Supplemental Comments in response to the Supplemental Advance Notice Of Proposed Rulemaking Order (ANOPR or Order) dated April 24, 2025 on Amendments to 52 Pa. Code §§ 57.11, 59.11, 61.11, and 65.2 in the above referenced docket.

Should you have any questions, please do not hesitate to contact the undersigned at (724) 416-6321.

Very truly yours,

Emily Farah

/kak
Enclosure
Cc Colin Scott, Assistant Counsel, Law Bureau colinscott@pa.gov
Chris Van de Verg, Assistant Counsel, Law Bureau cvandeverg@pa.gov
Daniel Searfoorce, Manager (BTUS) dsearfoorc@pa.gov
Michael Holko, Director, Cybersecurity Compliance 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	:	L-2022-3034353

SUPPLEMENTAL COMMENTS OF COLUMBIA GAS OF PENNSYLVANIA, INC.
TO SUPPLEMENTAL ADVANCE NOTICE OF PROPOSED RULEMAKING ORDER

I. INTRODUCTION

On November 10, 2022, the Pennsylvania Public Utility Commission ("PUC" or "Commission") entered an Advance Notice of Proposed Rulemaking Order ("ANOPR") to seek public comment on the sufficiency of current PUC regulations relating to cybersecurity. The Commission's cybersecurity regulations fall into two (2) groups: (1) cyberattack reporting[1] and (2) self-certification.[2]

On April 24, 2025, the Commission issued a Supplemental Advance Notice of Proposed Rulemaking Order ("Supplemental ANOPR") to request additional stakeholder feedback in light of several significant cybersecurity events and the United States Department of Homeland Security's ("DHS") Cybersecurity & Infrastructure Security Agency ("CISA") notice of proposed rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").

In Appendix A to the Supplemental ANOPR, the Commission further breaks down the

[1] *See* 52 Pa. Code §§ 57.11 (electric), 59.11 (natural gas), 61.11 (steam), and 65.2 (water).
[2] *See* 52 Pa. Code §§ 101.1 – 101.7 (jurisdictional utilities, which by definition do not include electric generation suppliers ("EGSs"), natural gas suppliers ("NGSs"), transportation network companies ("TNCs") or wastewater public utilities). *See also* 52 Pa. Code § 61.45 (steam).

foregoing topics into thirteen topics for comment.

Columbia Gas of Pennsylvania, Inc. ("Columbia") supports the supplemental comments submitted by the Energy Association of Pennsylvania ("EAP") at this docket. Columbia submits the within Supplemental Comments to provide additional information and recommendations on the thirteen topics for comment. Generally, however, Columbia maintains that the current regulations are appropriate to meet the Commission's goals without unnecessary duplication with the requirements of the federal government and other agencies. As such, minimal changes should be considered by the Commission, including the minor changes identified herein. To the extent any other changes are deemed necessary, they should be carefully crafted to provide value to this Commission's goals without creating additional burden and cost to utilities (and ultimately, ratepayers).

II. SUPPLEMENTAL COMMENTS

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?

Should the Commission require utilities to maintain cybersecurity programs, such programs should align with the National Institute for Standards and Technology ("NIST") frameworks, as they are commonly leveraged throughout the utility industry. For instance, Columbia leverages the NIST Cybersecurity Framework ("CSF") because it is a federally recognized foundational framework for establishing and maintaining cybersecurity controls and is adaptable to many other regulations. NIST Special Publication 800-53 and NIST Special Publication 800-82 are much more detailed and focused control frameworks that may be too granular and extensive for universal adoption.

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?

Yes. While Columbia cannot represent the views of smaller utilities, the Company recognizes that there is a significant financial burden on any company that maintains compliance with frameworks like NIST CSF. Further, due to the rapidly changing cyber security threats, needs and associated costs related to cybersecurity issues, the Commission should consider implementing alternative recovery mechanisms such as trackers to support timely implementation and maintenance of cybersecurity protections for all utilities.

Regarding the criteria the Commission may use to differentiate among utilities to determine the extent of a particular utility's obligations, Columbia recommends that the Commission consider the number of critical facilities[3] that the utility serves.

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

Should the Commission allow waivers, Columbia supports a very specific and defined set of criteria by which the Commission would evaluate such petitions. It is imperative that the Commission promulgate clearly defined exception criteria to ensure consistent application of any exception(s). For instance, one of the components the Commission should consider is the number of critical

[3] *See Pipeline Security Guidelines*, Table 1: Critical Facility Criteria (Transp. Sec. Admin. Mar. 2018, with Change 1 Apr. 2021), https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf at pp. 10-15.

facilities that the utility serves.

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?

No. Columbia submits that allowing utilities to opt out of using the uniform frameworks, like NIST CSF, risks undermining the consistency of federally recognized safeguards. While alternative programs may appear comparable, allowing deviations could prevent uniform oversight or enforcement. Additionally, the Commission's personnel may not have the requisite expertise to effectively manage enforcement for a variety of cybersecurity plans or frameworks.

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?

While Columbia cannot represent the views of smaller utilities, the Company supports the Commission allowing waivers for utilities that do not serve critical facilities, as indicated in 2(b), *supra*.

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

Columbia recommends incorporating by reference the most recently published version of NIST CSF or other federally accepted cybersecurity framework to allow the Commission's regulations to automatically reflect the latest technical developments and industry standards.

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

For jurisdictional utilities, Columbia submits that the Commission should accept a Public Utility Security Planning and Readiness Self-Certification Form ("SCF"). *See* 52 Pa. Code §§ 101.1-

101.7. Columbia maintains its position that the Commission should also require non-utility companies under the Commission's oversight to certify their cybersecurity fitness. As such, Columbia submits that suppliers should also be required to submit a SCF or a verified attestation that a self-assessment was completed.

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

Columbia recommends that the Commission, through the Bureau of Investigation and Enforcement ("I&E"), leverage the existing regulatory framework that allows filing a Formal Complaint to prosecute any violation of the Public Utility Code or Commission regulations. Further, any penalties that proposed by I&E would be subject to review under the standards set forth by *Rosi Pa. P.U.C. v. NCIC Operator Services*, M-00001440 (Order entered December 21, 2000).

3. Should an annual certification by a public utility that 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).

Yes. The Transportation Security Administration ("TSA") considers independent certification reports to the TSA Security Directives to be Security Sensitive Information ("SSI"), as that term is defined by 49 CFR 1520.5. Protections and protocols for SSI are similar to the protections for CSI.[4].

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?

Columbia recommends that the Commission collaborate with CISA or other federal agencies

[4] *See* 49 CFR 1520.9; 35 P.S. § 2141.3.

that accept SSI information to determine best practices and implement a solution that is validated by an independent assessment to ensure that the Commission has the ability to securely store information.

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?

No. While both the Commission's statutory purpose and CISA's NOPR contribute meaningful value, their core purposes differ. CISA centers its efforts on cultivating awareness and facilitating learning from historical cyber events, thereby serving as an organization that guides industry's best practices and creates a proactive environment through shared knowledge. In contrast, the Commission is focused on driving service performance and minimizing the impact on customers.

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

Broadly, Columbia submits that the Commission can provide customers with the most protection against cybersecurity attacks though proper policies and rate structures that encourage jurisdictional utilities to identify, protect, detect, respond and recover from cyberattacks. Due to the rapidly changing threats, needs and associated costs related to cybersecurity issues, the Commission should consider implementing alternative recovery mechanisms such as trackers to support timely implementation of cybersecurity measures.

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)).

None. Because this function is already being performed by the federal government through DHS and CISA, as well as the Information Sharing and Analysis Centers ("ISACs"), the Commission need not duplicate efforts by specialized federal agencies that possess the subject-matter expertise to oversee this function comprehensively.

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

None. Because this function is already being performed by the federal government through the DHS and the CISA, as well as ISACs, the Commission need not duplicate efforts by specialized federal agencies that possess the subject-matter expertise to oversee this function comprehensively.

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).

None. Because this function is already being performed by the federal government through the DHS and the CISA, as well as ISACs, the Commission need not duplicate efforts by specialized federal agencies that possess the subject-matter expertise to oversee this function comprehensively.

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).

None. Because this function is already being performed by the federal government through the DHS and the CISA, as well as ISACs, the Commission need not duplicate efforts by specialized federal agencies that possess the subject-matter expertise to oversee this function comprehensively.

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).

None. Because this function is already being performed by the federal government through the DHS and the CISA, as well as ISACs, the Commission need not duplicate efforts by specialized federal agencies that possess the subject-matter expertise to oversee this function comprehensively.

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?

None. Because this function is already being performed by the federal government through the DHS and the CISA, as well as ISACs, the Commission need not duplicate efforts by specialized federal agencies that possess the subject-matter expertise to oversee this function comprehensively.

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

Columbia submits that no public utility should be exempt from reporting cyber incidents to federal agencies. Further, cyber incident reporting should not only be applicable to public utilities, but also applicable to suppliers and any other entity subject to the Commission's oversight.

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?

Columbia does not recommend a requirement to report incidents at the state level in addition to the required reporting at the federal level, as duplicative reporting creates unnecessary costs and delays without improving cyber security. Cyber security incidents are generally complex, so in the

hours after a confirmed attack, utility efforts should be primarily focused on containment and protection of utility assets and customer information rather than reporting.

If the Commission requires that companies also report cybersecurity incidents to the Commission, Columbia submits that the Commission should accept incident reports that comply with another agency's regulations. Columbia suggests that the Commission should establish a means by which the federal agency automatically notifies the Commission when a company under the Commission's jurisdiction reports a cybersecurity incident.

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?

Columbia anticipates the potential for regulatory duplication and/or overlap in the reporting context. As indicated above, reporting at both the state and federal level creates unnecessary costs and delays in the midst of a cyber security incident without improving security of utility assets or customer information. Additionally, Current PUC regulations require reporting of physical or cyberattacks that cause either or both an interruption of service or $50,000 in damages. *See* 52 Pa. Code § 57.11(b)(4). As such, if the incident caused an outage or damages of $50,000 or more, the Commission would already be notified of the incident.

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?

In the interest of regulatory efficiency and alignment with best practices, the Commission

should mandate adoption of existing, widely recognized, cybersecurity programs rather than developing separate or duplicative standards. Leveraging established protocols, such as NIST CSF, promotes alignment with industry's best practices, reduces implementation burdens, and drives consistency. Creating new, isolated frameworks is likely to create unnecessary complexity and increase costs.

GENERAL

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.

Columbia does not expect the elimination of the cybersecurity aspects of Chapter 101 of the PUC's regulations to have any impact.

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.*

Columbia submits that the costs or benefits associated with the Staff Working proposals may not be able to be uniformly quantified across all utilities or companies under the Commission's jurisdiction. For example, the cost of reporting a cybersecurity incident varies widely due to a number of factors, including the company size, whether the company is publicly traded, size and makeup of the company's customer base, among other things.

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.

As indicated, above, Columbia would welcome the opportunity to implement alternative recovery mechanisms to support timely implementation of cybersecurity protections.

III. CONCLUSION

Columbia Gas of Pennsylvania, Inc. thanks the Commission for this opportunity to submit these Supplemental Comments to the Supplemental ANOPR and respectfully requests that the Commission adopt Columbia's recommendations.

Respectfully submitted,

Emily M. Farah (ID #322559)
NiSource Corporate Services Company
121 Champion Way, Ste. 100
Phone: 724-416-6321
E-mail: efarah@nisource.com