



Candis A. Tunilo
Senior Counsel
Legal Department

800 N. Third Street
Suite 204
Harrisburg, PA 17102
Cell: 223-488-0794
ctunilo@nisource.com

February 8, 2023

VIA ELECTRONIC FILING

Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor North
P.O. Box 3265
Harrisburg, PA 17105-3265

**Re: Rulemaking to Review Cyber Security Self-Certification
Requirements and the Criteria for Cyber Attack Reporting
Docket No. L-2022-3034353**

Dear Secretary Chiavetta:

Enclosed for filing please find Columbia Gas of Pennsylvania, Inc.'s Comments in response to the Advance Notice of Proposed Rulemaking Order (ANOPR) dated November 10, 2022 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 (223) 488-0794.

Very truly yours,


Candis A. Tunilo

/kak

Enclosure

Cc Colin Scott, Assistant Counsel, Law Bureau colin.scott@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 : L-2022-3034353
Criteria for Cyber Attack Reporting

**COMMENTS OF COLUMBIA GAS OF PENNSYLVANIA, INC. TO
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) cyber attack reporting¹ and (2) self-certification².

The Commission’s self-certification regulations were promulgated in 2005 as the culmination of an effort to coordinate with the Pennsylvania Office of Homeland Security without replicating regulations that were already in place and required by the Federal government or other agencies.³ The Commission’s cyber attack reporting regulations for electric, natural gas and water public utilities were promulgated in 2011 in response to customer dissatisfaction to the service

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).

³ See *Rulemaking re Public Utility Security Planning and Readiness*, Docket No. L-00040166, Revised Final Rulemaking Order (Mar. 10, 2005).

restoration and public notice practices after Hurricane Ike interrupted electric service to more than 450,000 customers in 2008.⁴ These regulations were intended to “establish a more uniform approach to reportable accidents involving utility facilities and operations.”⁵

In the ANOPR, the PUC requests feedback on the following:

- Updating terms and concepts;
- Approaches to ensuring cyber security fitness in public utilities;
- Improving the Self-Certification Form (“SCF”) process,
- Updating cyber attack reporting regulations;
- Merging the self-certification and cyber attack reporting regulations;
- The cost-benefit analysis of the forgoing items; and
- Eliminating regulatory duplication and overlap.

In Appendix A to the ANOPR, the Commission further breaks down the foregoing topics into fifteen numbered “topics for comment.”

Columbia Gas of Pennsylvania, Inc. (“Columbia”) supports the Comments submitted by the Energy Association of Pennsylvania (“EAP”) at this docket. Columbia submits these Comments to provide additional information and recommendations on two (2) specific topics identified in the ANOPR. Generally, however, Columbia submits 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

⁴ Cyber attack reporting regulations for steam utilities were promulgated in 2017. *See Final Rulemaking Re Steam Heat Distribution System Safety Regulations*, Docket No. L-2015-2498111, Final Rulemaking Order (Aug. 3, 2017).

⁵ *See Proposed Rulemaking for Revision of 52 Pa. Code Chapters 57, 59, 65 and 67 Pertaining to Utilities’ Service Outage Response and Restoration Practices*, Docket No. L-2009-2104274, Final Rulemaking Order (Sept. 23, 2011) at 2.

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. COMMENTS

A. Approaches to Ensuring Cybersecurity Fitness in Public Utilities.

In the ANOPR, the Commission identifies five (5) potential regulatory approaches to ensuring that public utilities have adequate cybersecurity plans in place: (1) self-certify annually to the PUC that the utility's plan, program or both complies with the PUC's regulations and is updated and tested annually; (2) self-certify annually to the PUC that the utility's plan, program or both complies with the appropriate Federal or industry standard and is updated and tested annually; (3) third-party expert certification annually to the PUC that the utility's plan, program or both complies with the appropriate Federal or industry standard and is 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 (5) require public utilities to file a confidential copy of cybersecurity plans and programs with the PUC for direct review and comment. *See* ANOPR at 12-13. The Commission seeks comment on the merits and weaknesses of these approaches in providing the PUC, public utilities and ratepayers with the greatest potential assurance that the utility is adequately prepared to address cybersecurity threats. *Id.* at 13.

Columbia submits that the first approach – annual self-certification to the PUC that the utility's plan, program or both complies with the PUC's regulations and is updated and tested annually – is preferable because the process has existed for many years and is well known.

Additionally, this process does not invoke unnecessary costs or burdens on utilities that must also comply with more stringent Federal requirements.

Columbia proposes, however, that the self-certification requirement be applicable to additional types of entities subject to the PUC's supervision, including but not limited to, electric generation suppliers ("EGSs") and natural gas suppliers ("NGSs") (collectively, "suppliers"). Utilities share information with EGSs and NGSs for many purposes, such as Purchase of Receivables programs. Utilities also rely on EGSs and NGSs for commodity to serve the utilities' customers. A cyber attack on an EGS or NGS is very likely to also affect the utilities, with which the supplier has commercial relationships, whether it be releasing customer personal identifying information, interrupting flow of commodity or some other issue. As such, to the extent the PUC also supervises suppliers, the PUC should require suppliers to certify their cybersecurity fitness in order to further the Commission's objectives in its regulations.

Additionally, Columbia submits that the Commission's regulations should not provide exemptions to the self-certification requirement. A cyber incident can impact the Commission, other utilities and ratepayers regardless of the size of the business involved. In fact, it is not uncommon for cyber incidents to originate from smaller companies that are engaged with larger companies. In order to provide additional assurance that utilities are adequately prepared to address cybersecurity threats, *all* public utilities subject to the Commission's jurisdiction should be required to comply with the cybersecurity self-certification requirement.

If, however, the Commission opts to implement the second approach – annual self-certification to the PUC that the utility's plan, program or both complies with the appropriate Federal or industry standard and is updated and tested annually – Columbia submits that the PUC must clarify what is meant by "Federal or industry standard." There are inconsistencies among

Federal standards, including specifically the definitions utilized by the North American Electric Reliability Corporation (“NERC”) in its Critical Infrastructure Protection Standards (“CIP”), the National Institute for Standards and Technology (“NIST”) and the TSA Security Directives. Additionally, public utilities may not have the technology and controls implemented to comply with any or all of the Federal standards. The cost to implement such technology and controls would be significant, and it is not likely that such requirement would further the PUC’s goals regarding cybersecurity.

Columbia submits that the remaining approaches identified by the Commission should be rejected. These approaches are quite invasive to utilities and increase the risk of inadvertent release of confidential plans or plan components. Further, any requirement for submission of plans to the PUC that includes uploading such plans into any PUC digital platform creates an opportunity for cybersecurity attack on all utilities simultaneously by merely attacking the PUC’s IT system. There is no benefit to this approach that outweighs this risk. Further, implementation of the third, fourth or fifth approach would involve significant time and costs for many utilities, as well as the PUC, without providing additional assurance that utilities are adequately prepared to address cybersecurity threats.

For the foregoing reasons, Columbia reiterates its preference that the PUC continue with the current requirement for annual self-certification to the PUC that the utility’s plan, program or both complies with the PUC’s regulations and is updated and tested annually. Further, Columbia submits that the cybersecurity regulations should be applicable to suppliers and any other entity subject to the Commission’s supervision. Finally, Columbia submits that no public utilities should be exempt from these regulations.

B. Updating Cyber Attack Reporting Regulations.

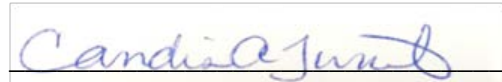
Currently, the PUC's regulations require the immediate reporting of physical or cyber attacks that cause either or both an interruption of service or \$50,000 in damages. *See e.g.* 52 Pa. Code § 57.11(b)(4). Columbia submits that the immediate reporting requirement is vague. Rather than "immediate" reporting, utilities should be provided at least seventy-two (72) hours to report a confirmed attack. Cybersecurity 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. On the other hand, a longer reporting timeframe, such as seventy-two (72) hours, will not reduce the Commission's role in cybersecurity.

Further, Columbia submits that it would be more appropriate to require that only "confirmed" physical or cyber attacks be reported rather than all attacks that cause either or both an interruption of service or \$50,000 in damages. In fact, the reporting requirement should not include any monetary threshold, as no such threshold exists in the Federal requirements. Instead, Columbia submits that the threshold should be based on impact, such as the attack's disruption to business functions.

III. CONCLUSION

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

Respectfully submitted,



Candis A. Tunilo (ID #89891)
NiSource Corporate Services Company
800 N. Third Street, Suite 204
Harrisburg, PA 17102
Phone: 717-233-1351
E-mail: ctunilo@nisource.com

Theodore J. Gallagher (ID # 90842)
NiSource Corporate Services Company
121 Champion Way, Suite 100
Canonsburg, PA 15317
Phone: 724-809-0525
E-mail: tjgallagher@nisource.com

Date: February 8, 2023

*Attorneys for Columbia Gas of
Pennsylvania, Inc.*

CERTIFICATE OF SERVICE

I hereby certify that true and correct copies of the foregoing have been served upon the following persons, in the manner indicated, in accordance with the requirements of § 1.54 (relating to service by a participant).

VIA E-MAIL ONLY

Richard A. Kanaskie, Esquire
Bureau of Investigation & Enforcement
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor
Harrisburg, PA 17120
rkanaskie@pa.gov

NazAarah Sabree, Small Business Advocate
Office of Small Business Advocate
555 Walnut Street
1st Floor, Forum Place
Harrisburg, PA 17101-1923
ra-sba@pa.gov
tereswagne@pa.gov

Patti Kay Wisniewski
Drinking Water Security/Preparedness
Coordinator
Drinking Water Section
U.S. Environmental Protection Agency
Four Penn Center
1600 John F Kennedy Blvd
Philadelphia, PA 19103-2852
Wisniewski.patti-kay@epa.gov

Christopher M. Andreoli
Darryl A. Lawrence
Office of Consumer Advocate
555 Walnut Street, 5th Floor
Forum Place
Harrisburg, PA 17101-1923
CAndreoli@paoca.org
DLawrence@paoca.org

Kevin Sunday
Director, Government Affair
PA Chamber of Business and Industry
417 Walnut Street
Harrisburg, PA 17101
ksunday@pachamber.org

Brandon Pierce, Esquire
PECO Energy Company
2301 Market Street
Suite 15
Philadelphia, PA 19103
Brandon.pierce@exeloncorp.com

Donna M.J. Clark
Vice President & General Counsel
Energy Association of PA
800 N. Third Street, Suite 205
Harrisburg, PA 17102-2025
dclark@energypa.org
nluciano@energypa.org

Darsh Singh, Esq.
First Energy / Met-Ed
2800 Pottsville Pike
P.O. Box 16001
Reading, PA 19612
singhd@firstenergycorp.com

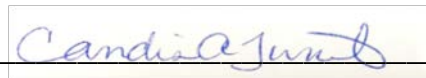
Pamela C. Polacek
CT Enterprises, Inc.
1775 Industrial Blvd.
Lewisburg, PA 17837
ppolacek@ctenterprises.org

Kimberly A. Klock
PPL
Two North Ninth Street
Allentown, PA 18101-1179
kklock@pplweb.com

Lindsay A. Baxter
Duquesne Light Company
411 Seventh Avenue, MailDrop 15-7
Pittsburgh, PA 15219
lbaxter@duqlight.com

Meagan B. Moore, Esq.
Peoples Companies
375 North Shore Drive
Pittsburgh, PA 15212
Meagan.moore@peoples-gas.com

February 8, 2023

A rectangular box containing a handwritten signature in blue ink that reads "Candis A. Tunilo".

Candis A. Tunilo
Counsel for Columbia Gas of Pennsylvania,
Inc.