ENTERPRISES, INC.

1775 Industrial Blvd. ● Lewisburg, PA 17837
Phone: 570-524-2231 ● Fax: 570-524-5887

Pamela Polacek, Chief Legal & Regulatory Officer
Direct Mail: P.O. Box 129; Venetia PA 15367
Direct Phone: 570-724-9469 (o); 717-503-6531 (m)
ppolacek@ctenterprises.org

February 8, 2023

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

VIA E-FILING

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 with the Pennsylvania Public Utility Commission ("PUC" or "Commission") are the Comments of Citizens' Electric Company of Lewisburg, PA, Wellsboro Electric Company and Valley Energy, Inc., regarding the above-referenced proceeding.

This filing has been served via email on the parties listed on the attached Certificate of Service. If you have any questions regarding this filing, please feel free to contact the undersigned. Thank you.

Very truly yours,

Pamela C. Polacek

By
Pamela C. Polacek

Counsel to Citizens' Electric Company of Lewisburg, PA,
Wellsboro Electric Company and Valley Energy, Inc.

Enclosure
c: Certificate of Service
Colin Scott, Esq., Assistant Counsel, Law Bureau (via email)
Chris Van de Verg, Esq., Assistant Counsel, Law Bureau (via email)
Daniel Searforce, Manager—Water, Reliability and Emergency Preparedness, TUS (via email)
Michael Holko, Director, Office of Cybersecurity Compliance and Oversight (via email)
Karen Thorne, Regulatory Review Assistant, Law Bureau (via email)

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

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

COMMENTS OF CITIZENS' ELECTRIC COMPANY OF LEWISBURG, PA, WELLSBORO ELECTRIC COMPANY AND VALLEY ENERGY, INC.

On November 10, 2022, the Pennsylvania Public Utility Commission ("PUC" or "Commission") issued an Advance Notice of Proposed Rulemaking Order ("ANOPR Order") seeking stakeholder input on a variety of issues regarding the Commission's existing cyber security self-certification requirements and criteria for reporting cyber attacks. The ANOPR Order was published in the *Pennsylvania Bulletin* on December 10, 2022.[1] Pursuant to the schedule set forth in the ANOPR Order, Citizens' Electric Company of Lewisburg, PA ("Citizens'"), Wellsboro Electric Company ("Wellsboro") and Valley Energy, Inc. ("Valley") (collectively, the "C&T Utilities" or "Companies") hereby submit these Comments.[2]

The C&T Utilities appreciate this opportunity to provide input as the Commission is in its initial stages of evaluating the self-certification and cyber attack reporting regulations. By its nature, cybersecurity is an ever-evolving aspect of utility operations. The C&T Utilities access cybersecurity expertise through a "shared service" arrangement that makes a six-member Information Technology and Cybersecurity department available to all operating companies in the C&T Enterprises, Inc., corporate family. Each of the operating companies also undertakes

[1] 52 Pa. Bull.7507.
[2] The C&T Utilities also join in and endorse the Comments submitted by the Energy Association of Pennsylvania.

company-specific efforts based on their unique network and equipment configurations. The cybersecurity plans are evaluated periodically to ensure that current threats are adequately and proactively addressed. The C&T networks undergo regular scanning and testing under the plans.

The C&T Utilities understand the Commission's desire to ensure that regulated entities are considering cybersecurity needs, just like the utility must consider other needs such as physical security, business continuity plans and emergency response plans. Our companies view the obligation to review and self-certify that we have appropriate plans in place as an important regulatory compliance activity. Our self-certification is then confirmed by the Commission in periodic management audits where the Commission's Bureau of Audits confirms that we maintain the required cybersecurity, business continuity, physical security and emergency response plans.

The ANOPR lists 15 specific questions for stakeholder input. The C&T Utilities respectfully submit that the first question is appropriate and, when considered, will resolve the Commission's inquiry. Specifically, Question 1 asks whether the existing self-certification and cyber attack reporting regulations are sufficient. The existing requirements ensure that the Commission knows the status of a utility's various emergency plans (cybersecurity, physical security, business continuity and emergency response), while also leaving the details of those plans in the hands of the utility management and boards of directors, where it rightly lies.

As the Commission is aware, Pennsylvania courts have long recognized that the day-to-day operational decisions of a utility must be left to the discretion of its management and board of directors.

> As explained by the Pennsylvania Supreme Court under the management decision doctrine 'it is not within the province of the Commission to interfere with the management of a utility unless an abuse of discretion or arbitrary action by the utility has been shown.'

Pickford v. Pa. Pub. Util Comm'n, 4 A.3d 707, 715, 2010 Pa. Commw. LEXIS 505, 202 (Pa Commw. 2010) (*citing Pa. Pub. Util. Comm'n v. Pennsylvania Electric Company*, 522 Pa. 338, 344, 561 A.2d 1224, 1226-27(1989). In *Pickford*, the Court upheld Pennsylvania American Water Company's discretion to chose between water treatment methods as part of PAWC's managerial discretion. *Id*. Similarly, the choices among various potential components of a cybersecurity plan is a managerial decision.

There is no "one size fits all" solution for cybersecurity. Each entity must evaluate the risks to its customers and enact strategies to counter the specific risks. Risk assessment includes the examination of many items, such as the potential sources for breaches, the likelihood of a particular type of breach and the consequences of a potential breach. For breaches that could result in utility service interruption, the assessment also includes the availability of back-up actions such as manual equipment operation or resets to counteract the initial disruption of utility service. In this respect smaller utilities such as the C&T Utilities that are not part of the bulk power or gas system face a different landscape than larger utilities with more interaction in the bulk systems. Some portions of utility operations can be segmented and isolated from outside computer networks to enhance security against operational cyber attacks. Smaller, distribution-only utilities like the C&T Utilities may be better able to rely on the continued segmentation between IT and OT.

For the C&T Utilities, the more significant cybersecurity risks arise regarding customer data and potential ransomware attacks. We typically detect C&T systems being probed by outside entities every 2 to 3 seconds looking for vulnerabilities. The C&T entities undertake multiple strategies to guard against network intrusions, including frequent system scanning, monitoring reliable cyber industry sources for information on emerging threats and security

patches, multi-factor authentication, and employee education on topics like social engineering and other security threats. We also go through the Payment Card Industry ("PCI") certification process each year to establish our fitness to hold and transact consumer credit card data.[3] Finally, we are vigilant with our vendors, including our billing vendor, regarding its cybersecurity measures.

The C&T Utilities have crafted cybersecurity approaches that are tailored and appropriate for the threats our companies face, and we will evolve those approaches to meet future developments in the cybersecurity landscape. The appropriate role for the Commission is ensuring that each utility maintains a cybersecurity plan. The detailed elements of the plan are an operational decision, guided by the utility's management and board of directors, and tailored to the utility's specific risks and needs. The current system of self-certification recognizes the appropriate demarcation between the Commission's powers under the Public Utility Code and the items that are appropriately left to management discretion.

RESPONSES TO SPECIFIC QUESTIONS

As directed by the ANOPR, the C&T Utilities are providing responses to the questions that were included in Attachment A. The C&T Utilities reserve the opportunity to respond to items raised by other commentators in future submissions to the Commission.

Introduction

1. The PUC seeks comments from interested stakeholders, including members of the regulated industry, statutory advocates, the public, and any other interested parties about

[3] The payment card industry maintains a Security Standards Council with requirements, training, threat updates and other information for merchants that accept credit or debit card payments. https://www.pcisecuritystandards.org/

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. *See* ANOPR at 2.

Response: As set forth in the previous section of these Comments, the existing regulations are sufficient and represent the appropriate balance between the Commission's oversight and utility managerial discretion. If the Commission is going to consider modifications, any revisions must take into account a solid cost-benefit analysis, especially for small utilities, and must be flexible to enable each utility to adapt to changing and evolving threats.

Updating Terms and Concepts

2. The PUC seeks comment on whether and how to update the terms and concepts used in the existing regulations to better reflect the current cybersecurity landscape, Federal and industry standards and any revisions which may be adopted in this rulemaking. *See* ANOPR at 9.

Response: The C&T Utilities have no specific comments at this time; however, we ask the Commission to remain mindful that certain NERC and other Federal cybersecurity requirements may apply only to the larger electric and gas utilities, while smaller utilities are not covered because they do not interact with the bulk electric and gas systems. Adopting Federal definitions may be too stringent and impose unreasonable requirements on smaller Pennsylvania utilities.

Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities

3. The PUC seeks comment on the relative merits and weaknesses of each of the approaches within the heading "Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities" and which of these approaches, some combination of these approaches, or some other approach, provides the PUC, the utility and its ratepayers with the greatest potential assurance that a utility is adequately prepared to address cyber security threats. *See* ANOPR at 13.

Response: As explained above, the C&T Utilities support continuation of the current self-certification approach. We provide the following initial comments on the other approaches for the Commission's consideration:

a. **Self Certification**: 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 report annually to the PUC that such plans are/or programs exist and are updated and tested annually.
Comments: The C&T Utilities support this approach.

b. **Self Certification of Industry Standard**: 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.
Comments: The C&T Utilities are not subject to the Federal cybersecurity regimes and would not be able to use this option.

c. **Third-Party Certification**: require the utility to provide a third-party expert certification that the public utility has a plan, a program or both, in place that complies 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.
Comments: The C&T Utilities do not support third-party certification. Based on our understanding, third-party certification is often expensive and requires significant internal resource allocation to perform self-assessments for the third-party that could be better directed to actual network security issues.

d. **Utility Management Audit**: integrate an onsite review of cybersecurity measures, plans and programs into the PUC's management audit process and examine cybersecurity measures, plans and programs in place as part of the audit function.
Comments: During the C&T Utilities' most recent management audit, the auditors confirmed the Companies' compliance with the requirements to maintain cybersecurity, business continuity and other emergency response plans. The scope of this review was reasonable and appropriate.

e. **File Copy of Cybersecurity Plans and Programs for Review**: require the 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.
Comments: The C&T Utilities respectfully suggest that this option is flawed for multiple reasons. First, the substantive review exceeds the Commission's jurisdiction and powers because it directly implicates day-to-day management decisions. *See Pickford* at 715. Second, this approach would require internal resources to coordinate with the Commission staff on the review, which would divert attention from actual network security activities. Third, it seems inadvisable for the Commission to have in its internal possession the cybersecurity plans and programs of all of the regulated utilities. This centralized collection of the plans creates new and substantial security risks.

4. The PUC welcomes comments describing the approaches taken by other state public utility commissions to address public utilities' cybersecurity fitness and evaluating their respective costs and benefits. *See* ANOPR at 13.

Response: The C&T Utilities have no comments at this time; however, we ask the Commission to remain cognizant of potential differences the utility industry composition in various states (e.g., does the state have smaller, distribution-only utilities).

5. Would changes to the cybersecurity aspect of 52 Pa. Code § 101.3 impact the physical security, emergency response and/or business continuity aspects of the rule and/or Chapter 101 generally? The PUC seeks comment on the nature and extent of such foreseeable impacts and ways to address those impacts. *See* ANOPR at 13.

Response: As the C&T Utilities support continuation of the current approach, there would be no impacts on the other emergency response plans.

6. The PUC seeks comment on whether the self-certification regulations should be applied to additional types of entities that are subject to the PUC's supervision? *See* ANOPR at 13.

Response: The C&T Utilities take no position on this item at this time.

7. The PUC seeks comment as to whether there are public utility types which should be wholly or partially exempt from the self-certification, based on easing the regulatory burden on small businesses, or for other reasons. *See* ANOPR at 14.

Response: Self-certification is appropriate for our entities. At this time, the C&T Utilities take no position on exemptions for other entities.

Improving the Self-Certification Form (SCF) Process

8. The PUC seeks comment on ways to streamline and otherwise improve the filing, handling, and storage of SCFs. *See* ANOPR at 15.

Response: The C&T Utilities have no comments on this item.

9. The PUC seeks comment on whether and how to streamline the self-certification form, plan and reporting requirements to better calibrate the benefits of the existing regulations against the burdens they place on regulated entities, especially smaller utilities, and on PUC staff. *See* ANOPR at 15-16.

Response: As set forth above, the self-certification process is an appropriate method for confirmation of cybersecurity activities. The C&T Utilities would not oppose modifications to streamline the process.

Updating Cyber Attack Reporting Regulations

10. The PUC seeks comment on potential ways to revise the reporting criteria in its existing regulations, including the potential addition of new requirements for reporting incidents involving IT. *See* ANOPR at 17.

Response: The C&T Utilities take no position on this item at this time.

11. The PUC seeks comment with respect to the continuing efficacy of the $50,000 reporting threshold. *See* ANOPR at 17.

Response: The C&T Utilities take no position on this item at this time.

Merging the Self-Certification and Cyber Attack Reporting Regulations

12. The PUC seeks comment on the pros and cons of merging the self-certification and cyber incident reporting regulations into a single chapter of the Code, and otherwise eliminating unintended or unjustified inconsistencies in the existing regulations. *See* ANOPR at 18.

Response: The C&T Utilities take no position on this issue at this time.

Cost-Benefit Analysis

13. The PUC seeks comment on how best to justify revisions to the existing regulations under the Regulatory Review Act standards. In particular, the PUC seeks comment on how the costs and benefits associated with its existing regulations, and any revisions thereto, can be objectively quantified and evaluated.
See ANOPR at 19.

Response: The response to this question depends on what revisions the Commission intends to pursue. As previously mentioned in the response to #3, the existing requirements are not unduly burdensome; however, some of the proposed enhancements (e.g., third party certification, annual submission/review of programs and plans) would be burdensome and would not meet a cost-benefit threshold for implementation.

Eliminating Regulatory Duplication and Overlap

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

Response: The C&T Utilities have no comments at this time.

Other Matters

15. Finally, the PUC seeks comments as to any additional considerations that parties may wish to raise at this time relating to PUC oversight and regulation of public utilities and licensed entities as it relates to their cybersecurity fitness. *See* ANOPR at 21.

Response: The C&T Utilities have no comments at this time.

WHEREFORE, Citizens' Electric Company of Lewisburg, PA, Wellsboro Electric Company and Valley Energy, Inc., respectfully urge the Commission to incorporate these Comments in its consideration of whether to move forward with the formal rulemaking and consider the positions stated above as it develops the changes, if any, that the Commission will propose to the cybersecurity self-certification and reporting requirements.

Respectfully submitted,

Pamela C. Polacek

By_____

Pamela C. Polacek (PA ID. No. 78276)
Chief Legal and Regulatory Officer
C&T Enterprises, Inc.
P.O. Box 129
Venetia, PA 15367
Phone: (570) 724-9496; (717) 503-6531(c)
ppolacek@ctenterprises.org

Counsel to Citizens' Electric Company of Lewisburg, PA, Wellsboro Electric Company and Valley Energy, Inc.

Date: February 8, 2023

CERTIFICATE OF SERVICE

I hereby certify that I am this day serving a true copy of the foregoing document upon the participants listed below in accordance with the requirements of Section 1.54 (relating to service by a participant).

VIA E-MAIL

Steven C. Gray, Esq. Teresa Wagner Office of Small Business Advocate Forum Place 555 Walnut Street, 1st Floor Harrisburg, PA 17101 sgray@pa.gov tereswagne@pa.gov	Michael S. Swerling, Esq. Timothy K. McHugh, Esq. Jessica Rogers, Esq. UGI Corporation 460 N. Gulph Road King of Prussia, PA 19406 SwerlingM@ugicorp.com MchughT@ugicorp.com JRogers@ugi.com
Patrick Cicero, Esq. Office of Consumer Advocate 555 Walnut Street Forum Place - 5th Floor Harrisburg, PA 17101-1921 pcicero@paoca.org	Richard A. Kanaskie, Esq. Director and Chief Prosecutor Bureau of Investigation and Enforcement Commonwealth Keystone Building 400 North Street, 2 West Harrisburg, PA 17120 rkanaskie@pa.gov
David P. Zambito, Esq. Cozen O'Connor 17 North Second Street, Suite 1410 Harrisburg, PA 17101 dzambito@cozen.com	Kimberly A. Klock, Esq. Michael J. Shafer, Esq. PPL Services Corporation Two North Ninth Street Allentown, PA 18101 kklock@pplweb.com mjshafer@pplweb.com
Caroline Choi, Esq. PECO Energy Company 2301 Market Street Philadelphia, PA 19103 Caroline.Choi@peco-energy.com	Darsh Singh, Esq. FirstEnergy Service Company 2800 Pottsville Pike P.O. Box 16001 Reading, PA 19612-6001 singhd@firstenergycorp.com

Susan E. Bruce, Esq. Charis Mincavage, Esq. McNees Wallace & Nurick LLC 100 Pine Street Harrisburg, PA 17101 sbruce@mcneeslaw.com cmincavage@mcneeslaw.com *Counsel to PECA*	Donna M.J. Clark, Esq. Energy Association of Pennsylvania 800 North Third Street Suite 205 Harrisburg, PA 17102 dclark@energypa.org
Amy E. Hirakis, Esq. Candis Tunilo, Esq. Nisource Corporate Services Co. 800 N. Third Street Harrisburg, PA 17102 ahirakis@nisource.com ctunilo@nisource.com	Theodore J. Gallagher, Esq. Assistant General Counsel Nisource Corporate Services Co. 121 Champion Way, Suite 100 Canonsburg, PA 15317 tjgallagher@nisource.com
Pennsylvania Utility Law Project 118 Locust Street Harrisburg, PA 17101 pulp@pautilitylawproject.org	Lindsay Baxter Duquesne Light Company 411 Seventh Avenue, 15-7 Pittsburgh, PA 15219 lbaxter@duqlight.com
Derrick Price Williamson, Esq. Barry A. Naum, Esq. Spillman Thomas & Battle 1100 Bent Creek Blvd, Suite 101 Mechanicsburg, PA 17050 dwilliamson@spillmanlaw.com bnaum@spillmanlaw.com *Counsel to IECPA*	Elizabeth R. Triscari, Esquire Pennsylvania American Water Company 852 Wesley Drive Mechanicsburg, PA 17055 Elizabeth.triscari@amwater.com
Andrew Wachter, Esq. Peoples Gas Company 375 North Shore Drive, Suite 600 Pittsburgh, PA 15212-5866 Andrew.wachter@peoples-gas.com	Dominick A. Sisinni, Esq. National Fuel Gas Distribution Corp. 1100 State Street Erie, PA 16501 SisinniD@natfuel.com
Steve Samara Pennsylvania Telephone Association 30 N. 3rd Street, Suite 300 Harrisburg, PA 17101 Steve.Samara@patel.org	Susan D. Paiva, Esq. Associate General Counsel Verizon 900 Race Street, 6th Floor Philadelphia, PA 19107 Susan.d.Paiva@verizon.com

Sue Benedek, Esq. CenturyLink 240 North 3rd Street, Suite 300 Harrisburg, PA 17101 Sue.Benedek@centurylink.com	Charles E. Thomas, III, Esq. Thomas Niesen & Thomas, LLC 212 Locust Street, Suite 302 Harrisburg, PA 17101-1510 Cet3@tntlawfirm.com *Pennsylvania Rural Telephone Coalition*

Pamela C. Polacek

Pamela C. Polacek (PA ID No. 78276)

Dated this 8th day of February, 2023, in Venetia, Pennsylvania.