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

July 16, 2025

Matthew Homsher, 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 Homsher:

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., on the Supplemental Advanced Notice of Proposed Rulemaking Order in 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)

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

Office of Small Business Advocate Forum Place 555 Walnut Street, 1st Floor Harrisburg, PA 17101 RA-SBA@PA.GOV	Allison Kaster Esq. Director and Chief Prosecutor Bureau of Investigation and Enforcement Commonwealth Keystone Building 400 North Street, 2 West Harrisburg, PA 17120 akaster@pa.gov
Office of Consumer Advocate 555 Walnut Street Forum Place - 5th Floor Harrisburg, PA 17101-1921 RA-OCA@PAOCA.ORG	

Pamela C. Polacek

Pamela C. Polacek (PA ID No. 78276)

Dated this 16th day of July, 2025, in Venetia, Pennsylvania.

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 SUPPLEMENTAL ADVANCED NOTICE OF PROPOSED RULEMAKING ORDER

On April 24, 2025, the Pennsylvania Public Utility Commission ("PUC" or "Commission") issued a Supplemental Advanced Notice of Proposed Rulemaking Order ("Supplemental ANOPR Order") seeking stakeholder input on a variety of issues regarding cyber security plans and incident reporting. The Supplemental ANOPR Order included a list of Topics for Comment and Staff Working Proposals. The Supplemental ANOPR Order was published in the *Pennsylvania Bulletin* on May 17, 2025.[1] Pursuant to the schedule set forth in the Supplemental 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 additional opportunity to provide input as the Commission is in the initial stages of evaluating the self-certification and cyber attack reporting regulations. The C&T Utilities understand the Commission's desire to ensure that regulated

[1] 55 Pa. Bull.3379.
[2] The C&T Utilities also join in and endorse the Comments submitted by the Energy Association of Pennsylvania.

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 cybersecurity as a key strategic planning objective.

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 are a managerial decision that should be respected by the Commission unless the utility engages in arbitrary conduct or abuses its discretion.

There is no "one size fits all" solution for cybersecurity. Each entity must evaluate the risks to its customers and enact cost-effective 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. As explained below, allowing the utility to align with an

established framework or set of standards can facilitate the reasoned evolution of an appropriate cybersecurity plan for their organization.

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. Aspects of the Staff Working Proposal go beyond this goal and provide overly rigid plan requirements. 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.

In addition, reporting requirements should be tailored to the Commission's oversight role on cybersecurity. The Supplemental ANOPR Order notes that the Commission, to date, has not "engaged in threat analysis, information sharing or assisting public utilities with incident response." Supplemental ANOPR Order, p. 17. As explained in the response to Question 5 below, the C&T Utilities urge the Commission to focus its reporting requirements on situations of actual harm, rather than the "risk for potential compromise."

RESPONSES TO SPECIFIC QUESTIONS

As directed by the Supplemental ANOPR Order, the C&T Utilities are providing responses to the Topics for Comment that were included in Attachment A. The C&T Utilities reserve the opportunity to respond to items raised by other stakeholders in future submissions to the Commission.

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?

RESPONSE: At this time, the C&T Utilities' cybersecurity efforts generally align with the NIST Cybersecurity Risk Framework ("CSF"). The CSF is a collection of guidance for entities; the CSF is not a checklist that will apply to every organization and situation. The alignment of an entity's cybersecurity program with the CSF must reflect the organization's risks and program maturity. The Commission's use of "conform" in this question appears to overlook the nature of the guidelines, transforming the CSF into an all or nothing compliance approach. Alignment with CSF should be considered a permissible program design option. The regulations should also permit the utility to designate an alternative framework or set of standards that may better fit the utility's organizational risks and needs.

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?***

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

   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?***

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?***

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

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

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

RESPONSE: As noted above, the CSF isn't a checklist for cybersecurity compliance. The Commission's review of cybersecurity efforts must take the nature of the CSF into account when evaluating each entity's cybersecurity program. This will enable the Commission to consider the utility's size, risks and program maturity in overseeing cybersecurity plans.

Although some general assumptions regarding cybersecurity risk can be made based on the organization's size, the risk-based approach should also focus on the types of facilities that the entity manages, the susceptibility to specific types of cybersecurity threats, the cost of counter-strategies and the potential harms that may result from a successful cybersecurity threat. As noted in the C&T Utilities' February 8, 2023 Comments on the Advanced Notice of Proposed Rulemaking Order, the C&T Utilities believe that the current self-certification process is sufficient, with the Commission's staff engaging in a more thorough review during the periodic Management Audit process. That review can consider whether particular standards or frameworks are reasonable based on the utility's size, type of assets and Personal Information ("PI") collection or storage practices and the utility's efforts to align with the self-designated standards.

The C&T Utilities appreciate the Commission's consideration of a waiver process for smaller utilities. For many regulatory requirements, filing a Petition for Waiver is an efficient method to accommodate smaller utility risks and resources. In this instance, however, we respectfully urge the Commission to also adjust the appropriate placement of smaller utilities with no critical infrastructure within the proposed compliance classes. A utility serving less than 100,000 customers that does not have bulk electric system assets and/or other critical infrastructure under the Federal definitions should be classified as a Class 3 utility. This change will enable the Commission to use the Class 2 requirements for smaller utilities with heightened risks due to the ownership of bulk electric facilities and/or other critical infrastructure, while maintaining appropriate Class 3 oversight for smaller utilities that do not have those facilities.

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

   RESPONSE: Yes, the form should continue to be considered CSI.

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?***

   RESPONSE: The self-certification should be a very short confirmation that a cybersecurity plan is maintained and available at the utility's offices.

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?

RESPONSE: The C&T Utilities support an incident reporting process that is tailored to the potential public harms of cybersecurity breaches. The nature of the public harm is proportionate to the ratepayer impacts that may be experienced if a particular entity's systems are breached. The C&T Utilities urge the Commission to focus on actual breaches, rather than situations where the utility's countermeasures have thwarted the system intrusion (or PI exfiltration) attempt. Section 102(a)(iv) of the Staff Working Proposals should be eliminated, as it focuses on the "risk for potential compromise of IT or OT owned, controlled or managed by, or serving, entities other than the reporting public utility, including customers, third parties, the Commission or other public utilities," rather than being focused on actual compromise of the systems.

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

   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)).***

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

   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).***

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).***

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).***

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?***

RESPONSE: The C&T Utilities support the Commission's roles in items c, d and f; we do not support the roles in the list that would duplicate Federal and law enforcement efforts. We appreciate receiving notices from the Commission to reinforce current threat trends as an additional source for our security monitoring.

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

RESPONSE: If the reporting obligations are appropriately tailored to represent situations of actual breach and harm to Pennsylvania consumers, then all public utilities (and competitive suppliers who serve Pennsylvania consumers in restructured industries) should be required to comply unless the event has already been reported to another regulatory entity.

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?***

RESPONSE: The C&T Utilities do not have a position on this item at this time.

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?***

RESPONSE: The C&T Utilities do not have a position on this item at this time.

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?***

RESPONSE: The C&T Utilities do not have a position on this item at this time.

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.***

RESPONSE: The C&T Utilities do not have a position on this item at this time.

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.***

RESPONSE: It is difficult at this time to objectively quantify the costs of the Staff Working Proposals. The costs would include both the time and resources to prepare new filings with the Commission and the costs that may be incurred if the Commission requires a utility to implement particular measures in the cybersecurity plan. For example, if the Commission mandates the frequency of tabletop exercises, then the costs could exceed those that utility would incur if each entity used its managerial discretion to engage in such strategies at self-determined frequencies based on their risk profile and the costs of the activities. In addition, the costs to comply with the regulations will depend on whether the Commission adopts the proposed classification modification discussed in the C&T Utilities' response to Question 13 below. If smaller entities are required to seek waivers to obtain compliance obligations that are more reasonable for their size and facility risks, then the costs to comply will increase. The C&T Utilities look forward to continuing to work with stakeholders and the Commission to evaluate this issue.

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.***

RESPONSE: Similar to many regulatory issues, the Commission's oversight of cybersecurity fitness and cyber incident reporting must strike an appropriate balance. The C&T Utilities respectfully suggest that aspects of the proposed regulations contained in the Supplemental ANOPR are overly prescriptive and may intrude on the utility's managerial discretion to design its cybersecurity program.

The C&T Utilities are classified as a Class 2 utility in the proposed regulations; however, the requirements set forth for a Class 1 or 2 utility are overly rigid and do not recognize the role of the utility's management and Board of

Directors in reviewing and overseeing utility operations. In contrast, the C&T Utilities view the proposed requirements for a Class 3 utility as better reflecting the appropriate balance for all utilities and while ensuring that critical program evaluation occurs and that response programs are in place. If the Commission believes that the Class 1 and 2 requirements are needed for some larger utilities, then the Class 3 requirements should be adopted for any utility that serves fewer than 100,000 customers and does not possess critical infrastructure or bulk electric system facilities.

The C&T Utilities also recommend changes to specific aspects of the requirements for Class 2 and Class 3 utilities that are unnecessarily rigid and do not allow each utility to adopt a program reflecting its individual risks and maturity.

i. Class 2 Proposed Requirements:

Aspects of the Class 2 requirements that are overly prescriptive include:

1. **A governance program**. The Staff Working Proposals define the governance program as: "The organizational mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements relating to cybersecurity. The governance program comprises governance policies and procedures, risk management strategies, defines oversight responsibilities for the public utility, and identifies individual roles, responsibilities, and authorities." The C&T Utilities support flexibility to enable each utility's management and Board of Directors to establish the contents of and governance for the cybersecurity program. Attempts to specify that the program include an "organizational mission, stakeholder expectations, dependencies and

legal regulatory and contractual requirements" removes management's discretion to adopt a program that is appropriate for the governance structure and culture of the organization. Moreover, any attempt to specify "contractual requirements" through a governance program ignores the nature of contractual negotiations and bargaining power, including the limited leverage that smaller entities may possess.

2. **A security management program**. The proposed regulations contain very specific requirements for the utility's mandatory security management program. For example, the program must ensure:
    - All confidential data is encrypted at rest and in transit.
    - All IT, OT, cloud, and physical access contracts with any third party are reviewed for compliance with applicable standards and to ensure that all potential vulnerabilities are identified and addressed as part of the contractual agreements and licenses.

First, regarding the proposed requirement for encryption of "all confidential data" at rest and in transit, the regulations do not distinguish between types of "confidential data" that may exist or between ways to safeguard access to confidential data that may involve strategies other than encryption. Utility personnel may exchange various types of confidential information,

including customer-specific usage or cost information, internal financial information and attorney-client privileged communications. This information generally is not encrypted when exchanged internally among employees that have a business need for the data and are subject to Company policies prohibiting non-disclosure of customer information (or business intelligence). In addition, it may be shared with outside professional services vendors such as auditors, accountants and attorneys that have fiduciary and confidentiality duties. Clearly, all utilities must protect confidential data; however, there may be methods other than encryption that can be used.

Second, the mandatory contents of the security plan presuppose the bargaining power of the utility to insist on contractual provisions with vendors for IT, OT, cloud and physical access contracts. In the C&T Utilities' experiences, the ability to request such changes is very limited.

3. **A risk management program**. –The proposed regulations require a "risk management program"; however, the regulations do not provide a definition for this element. It should be deleted from the list.

4. **A recovery management program**. The definition of "recovery management program" states that the cybersecurity program must include a

"resiliency policy and procedure"; however, this element is not defined in the proposed regulations. In addition, the definition of "recovery management program" requires yearly tabletop exercises. Each utility should determine the frequency and type of training that will occur based on its risk exposure and the costs/benefits of various training strategies. Mandating yearly tabletops clearly intrudes on the utility's managerial discretion.

ii. Class 3 Proposed Requirements

As previously explained, the requirements set forth for a Class 3 or 4 utility generally provide an appropriate balance between the Commission's oversight duties and the utility's managerial discretion to design and implement its cybersecurity program. Despite the C&T Utilities' general agreement with the requirements set forth for Class 3 or 4 utilities, the C&T Utilities do not agree with the concept that the cybersecurity plan and risk mitigation plan must be "updated annually to address the findings of the annual" NIST CSF and vulnerability assessment. The findings of those annual processes may identify risks that are of remote likelihood or would be extremely costly to mitigate. If that occurs, then the subsequent program should not be modified to address those risks.

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: July 16, 2025