Kimberly A. Klock
Assistant General Counsel

PPL
645 Hamilton Street, Suite 700
Allentown, PA 18101
Tel. 610.774.5696 Fax 610.774.4102
KKlock@pplweb.com

E-File

July 16, 2025

Matthew Homsher, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor North
Harrisburg, PA 17120-3265

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 on behalf of PPL Electric Utilities Corporation ("PPL Electric") are PPL Electric's Comments regarding the Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, pursuant to the Supplemental Advanced Notice of Public Rulemaking entered April 24, 2025, and published in the *Pennsylvania Bulletin* on May 17, 2025.

Copies have been served as indicated below and on the attached Certificate of Service.

Pursuant to 52 Pa. Code § 1.11, the enclosed document is to be deemed filed on July 16, 2025, which is the date it was filed electronically using the Commission's E-filing system.

If you have any questions, please do not hesitate to contact me.

Respectfully submitted,

Kimberly A. Klock

Enclosure

cc via email: Colin Scott, Law Bureau (colinscott@pa.gov)
Chris Van de Verg, Law Bureau (cvandeverg@pa.gov)
Karen Thorne, Law Bureau (kathorne@pa.gov)
Daniel Searfoorce, TUS (dsearfoorc@pa.gov)
Michael Holko, Office of Cybersecurity Compliance and Oversight (miholko@pa.gov)
Certificate of Service

CERTIFICATE OF SERVICE

(Docket No. L-2022-3034353)

I hereby certify that a true and correct copy of the foregoing has been served upon the following persons, in the manner indicated, in accordance with the requirements of 52 Pa. Code § 1.54 (relating to service by a participant).

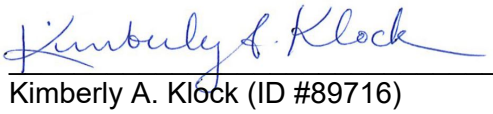
VIA ELECTRONIC MAIL

Darryl Lawrence, Esquire
Office of Consumer Advocate
555 Walnut Street, Forum Place, 5th Floor
Harrisburg, PA 17101-1923
dlawrence@paoca.org

Allison Kaster, Esquire
Bureau of Investigation & Enforcement
Commonwealth Keystone Building
400 North Street, 2nd Floor West
Harrisburg, PA 17105-3265
akaster@pa.gov

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

Date: July 16, 2025



Kimberly A. Klock (ID #89716)
Michael J. Shafer (ID #205681)
PPL Services Corporation
645 Hamilton Street, Suite 700
Allentown, PA 18101
Phone: (610) 774-5696
Fax: (610) 774-4102
Email: kklock@pplweb.com
Email: mjshafer@pplweb.com

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

COMMENTS OF
PPL ELECTRIC UTILITIES CORPORATION

I. INTRODUCTION

On November 10, 2022, the Pennsylvania Public Utility Commission ("Commission") entered an Advance Notice of Proposed Rulemaking Order ("ANOPR") at the instant docket. Through the ANOPR, the Commission requested "comments from interested stakeholders, including members of the regulated industry, statutory advocates, the public, and any other interested parties about 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." ANOPR, p. 2. PPL Electric Utilities Corporation ("PPL Electric" or the "Company") and other interested stakeholders submitted Comments on the ANOPR between January 30, 2023, and February 8, 2023.

Subsequently, on April 24, 2025, the Commission issued its Supplemental Advanced Notice of Proposed Rulemaking ("SANOPR") setting forth a list of additional questions on which the Commission seeks comments related to "whether the existing [cybersecurity] 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." SANOPR, p. 5. The SANOPR directed interested parties to file Comments within 60 days following publication in the *Pennsylvania Bulletin*. The SANOPR was published in the *Pennsylvania Bulletin* on May 17, 2025. Accordingly, Comments are due by July 16, 2025.

PPL Electric supports the Commission's efforts to update its cybersecurity regulations and appreciates the opportunity to provide comments to the Commission regarding the additional cybersecurity issues identified in the SANOPR.

II. PPL ELECTRIC'S COMMENTS

A. 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?

PPL Electric believes that requiring utilities to conform to the NIST Cybersecurity Risk Framework would provide a structured approach across all jurisdictional utilities to manage cyber risks and would help utilities align cybersecurity with business strategy and objectives. However, requiring conformity to NIST Special Publications 800-53 and 800-82 specifically could prove both challenging and costly for utilities. While Special Publication 800-53 provides comprehensive security and privacy controls, conformance could be burdensome due to the extensive list of controls included and would require significant effort to implement and ensure continual compliance. Special Publication 800.82, which is specific to securing Operational Technology ("OT") systems, could also be challenging to implement because it requires specialized skills and expertise and may not be adaptable to all frameworks.

PPL Electric respectfully recommends that the Commission consider adopting or aligning any standards adopted with the "CYBERSECURITY BASELINES FOR ELECTRIC DISTRIBUTION SYSTEMS AND DER" that were developed by the National Association of Regulatory Utility Commissioners ("NARUC") and the U.S. Department of Energy ("DOE") ("NARUC/DOE Baselines"). Although the NARUC/DOE Baselines were tailored primarily for distribution standards, these standards were based on the U.S. Department of Homeland Security

("DHS") and the Cybersecurity and Infrastructure Security Agency ("CISA") cybersecurity baselines and were developed to help public utility commissions keep security recommendations and the implementation of such recommendations consistent across states. PPL Electric believes that aligning any Commission standards with the NARUC/DOE Baselines will help provide consistency to utilities operating in multiple states.

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?

PPL Electric generally supports taking into consideration the impact that requiring conformity to cybersecurity standards would have on utilities across the industry, both operationally and financially. For example, the Commission could consider criteria including the number of customers in the utility's service area, the size of the company, the type of service provided (e.g., gas, electric), the federal cybersecurity-related regulations with which the utility must comply, and a utility's cybersecurity hygiene. However, PPL Electric's overarching concern is that any standards adopted by the Commission should be consistent with the existing regulatory cybersecurity requirements for utilities, many of which have unique disclosure and reporting requirements as well as other mandates. As such, PPL Electric recommends that the Commission consider the existing frameworks that utilities must follow, such as the North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") standards. PPL Electric cautions that adding additional frameworks could result in unnecessary complexity and costs to utilities without providing corresponding benefits.

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

The Company does not believe it is necessary for the Commission to specify the criteria it would consider in a petition to waive its cybersecurity requirements. Section 5.43 of the Commission's regulations already sets forth the procedural and substantive requirements for utilities seeking a waiver of the Commission's regulations. *See* 52 Pa. Code § 5.43. Indeed, a petition for waiver must: (1) "set forth clearly and concisely the interest of the petitioner in the subject matter, the specific regulation, amendment, waiver or repeal requested"; (2) "cite by appropriate reference the statutory provision or other authority involved"; and (3) "set forth the purpose of, and the facts claimed to constitute the grounds requiring the regulation, amendment, waiver or repeal." *Id.* § 5.43(a). PPL Electric believes that a utility seeking waiver of cybersecurity requirements can proceed under this existing regulation and that setting forth additional criteria specific to the proposed cybersecurity regulations is unnecessary.

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?

Yes. As stated in the Company's response to Question 2.b, above, PPL Electric maintains that Section 5.43 of the Commission's regulations already provides a clear path for utilities to request waivers of Commission regulations, which could be used to request a waiver allowing 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?

PPL Electric has no comment on this section of the SANOPR.

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

PPL Electric has no comment on this section of the SANOPR.

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

PPL Electric has no comment on this section of the SANOPR.

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

PPL Electric has no comment on this section of the SANOPR.

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).

Under the current regulatory framework, PPL Electric submits an annual self-certification form pursuant to 52 Pa. Code § 101.4(a). Per Section 101.5 of the Commission's regulation, this self-certification form "is not a public document or record and is deemed confidential and proprietary." 52 Pa. Code § 101.5. PPL Electric supports a heightened level of protection of the annual self-certification, particularly if changes are made through this rulemaking process that result in more detailed cybersecurity information being provided to the Commission. As for the process for submitting and protecting confidential security information ("CSI") from unwarranted disclosure, PPL Electric sees no reason to deviate from the Commission's established practices for the treatment and protection of such information and materials.

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?

As explained in the prior section, PPL Electric sees no reason to deviate from the Commission's established practices for the treatment and protection of information and materials that constitute CSI.

B. 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?

The Commission plays a crucial role in regulating public utilities to ensure they provide adequate, efficient, safe, and reasonable service to Pennsylvania consumers and ratepayers. As administered by CISA, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") was enacted to help preserve national security, economic security, and public health and safety. CIRCIA seeks to increase the likelihood that critical infrastructure entities will be able to address identified vulnerabilities and be secure against threats. Although PPL Electric does not believe that CIRCIA's purpose and the Commission's statutory role are substantially the same, the Company recognizes that both CISA and the Commission seek to protect the public by ensuring to protect against various cyber threats and threat actors. To this end, the Commission's cybersecurity efforts are consistent with both the purpose of CIRCIA and the Commission's role in regulating public utilities in Pennsylvania.

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?

PPL Electric does not have specific responses to each of the subparts contained in Question 6. Generally, however, the Company agrees that the Commission should play a vital role in utility cybersecurity oversight. For example, the Commission should ensure that utilities are prepared to prevent and respond to cyber threats and events, provide trend and threat analysis, offer training for and assistance to utilities in terms of intelligence and awareness, and provide informational communications, including trend and threat advisories. In addition, the Commission should continue to collaborate with federal agencies to ensure the sharing of cyber and threat intelligence, particularly as related to critical infrastructure. As such, PPL Electric recognizes the unique role that the Commission can play in providing public utilities with the insight and tools necessary to identify and assess cybersecurity risk and trends and to help the industry improve incident response and mitigation.

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

PPL Electric does not support exempting certain types of fixed public utilities from the requirement to report cyber incidents. A cyber incident could impact critical infrastructure not isolated to one utility or type of utility. For example, cyber incidents impacting telecommunications and natural gas utilities could in turn affect an electric utility's ability to provide safe, reasonable, reliable, and adequate service. As such, to the extent reporting is required, PPL Electric respectfully recommends that all fixed utilities should be required to report cyber incidents.

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?

PPL Electric believes that the Commission should collaborate with other agencies to prevent the creation of overlapping, burdensome, or different reporting requirements. For example, the Company is already subject to existing Securities Exchange Commission ("SEC") cyber incident reporting requirements. Other federal regulations, such as CIRCIA's reporting requirements, have not yet been finalized but are expected to require the reporting of substantial cyber incidents and ransomware payments. Layering disparate reporting requirements on utilities without coordination between agencies or recognition of existing reporting obligations could unnecessarily increase compliance costs, reduce efficiency, or lead to conflicting requirements. Thus, PPL Electric respectfully recommends that the Commission collaborate with other agencies imposing cyber reporting requirements or take those requirements into consideration when developing its own standards in order to reduce regulatory overlap.

C. 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?

At this time, PPL Electric cannot definitively determine whether there would be overlap with the CISA's implementation of CIRICA, as those new federal regulations are due to be finalized by October 2025. However, as explained in the prior section, PPL Electric recommends that the Commission collaborate with other agencies, such as CISA, to avoid any potential overlapping regulatory requirements.

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?

As detailed in the Company's response to Question 8, PPL Electric believes that collaboration among agencies can help the Commission eliminate regulatory duplication or overlap. To the extent that agency collaboration is not feasible, PPL Electric respectfully recommends that the Commission consider implementing or adopting existing cybersecurity standards and frameworks already applicable to jurisdictional utilities, including reporting requirements, to prevent regulatory overlap.

D. 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.

PPL Electric has no comment on this section of the SANOPR.

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.

PPL Electric has no comment on this section of the SANOPR.

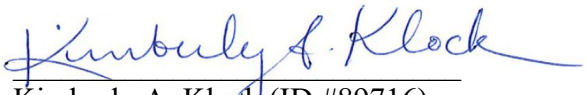
13. Comment as to any additional considerations that you may wish to raise at this time relating to PUC oversight and regulation of public utilities as it relates to their cybersecurity fitness and/or cyber incident reporting.

PPL Electric has no comment on this section of the SANOPR.

III. CONCLUSION

As stated above, PPL Electric supports the Commission's efforts to update the existing cybersecurity regulations and appreciates this opportunity to provide input on the SANOPR. PPL Electric looks forward to working with the Commission and other stakeholder as this process moves forward.

Respectfully submitted,



Kimberly A. Klock (ID #89716)
Michael J. Shafer (ID #205681)
PPL Services Corporation
645 Hamilton Street, Suite 700
Allentown, PA 18101
Phone: 610-774-5696
Fax: 610-774-4102
E-mail: kklock@pplweb.com
E-mail: mjshafer@pplweb.com

Date: July 16, 2025

Counsel for PPL Electric Utilities Corporation