

**Kimberly A. Klock**  
Assistant General Counsel

**PPL**  
Two North Ninth Street  
Allentown, PA 18101-1179  
Tel. 610.774.5696 Fax 610.774.4102  
KKlock@pplweb.com



**E-File**

February 8, 2023

Rosemary Chiavetta, Secretary  
Pennsylvania Public Utility Commission  
Commonwealth Keystone Building  
400 North Street, 2<sup>nd</sup> 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 Chiavetta:

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 Advanced Notice of Public Rulemaking entered November 10, 2022, and published in the *Pennsylvania Bulletin* on December 10, 2022.

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 February 8, 2023, 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 ([colin.scott@pa.gov](mailto:colin.scott@pa.gov))  
Chris Van de Verg, Law Bureau ([cvandeverg@pa.gov](mailto:cvandeverg@pa.gov))  
Karen Thorne, Law Bureau ([kathorne@pa.gov](mailto:kathorne@pa.gov))  
Daniel Searfoorce, TUS ([dsearfoorc@pa.gov](mailto:dsearfoorc@pa.gov))  
Michael Holko, Office of Cybersecurity Compliance and Oversight ([miholko@pa.gov](mailto: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

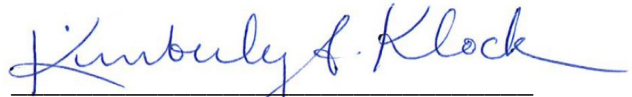
Patrick Cicero, Esquire  
Christopher Andreoli, Esquire  
Office of Consumer Advocate  
555 Walnut Street, Forum Place, 5th Floor  
Harrisburg, PA 17101-1923  
[pcicero@paoca.org](mailto:pcicero@paoca.org)  
[candreoli@paoca.org](mailto:candreoli@paoca.org)

Richard Kanaskie, Esquire  
Bureau of Investigation & Enforcement  
Commonwealth Keystone Building  
400 North Street, 2nd Floor West  
Harrisburg, PA 17105-3265  
[rkanaskie@pa.gov](mailto:rkanaskie@pa.gov)

NazAarah Sabree  
Teresa Wagner  
Office of Small Business Advocate  
555 Walnut Street  
Forum Place, 1<sup>st</sup> Floor  
Harrisburg, PA 17101  
[ra-sba@pa.gov](mailto:ra-sba@pa.gov)  
[tereswagne@pa.gov](mailto: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](mailto:Wisniewski.patti-kay@epa.gov)

Date: February 8, 2023



Kimberly A. Klock (ID #89716)  
Michael J. Shafer (ID #205681)  
PPL Services Corporation  
Two North Ninth Street  
Allentown, PA 18101  
Phone: (610) 774-5696  
Fax: (610) 774-4102  
Email: [kklock@pplweb.com](mailto:kklock@pplweb.com)  
Email: [mjshafer@pplweb.com](mailto:mjshafer@pplweb.com)

**BEFORE THE  
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

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

---

**COMMENTS OF  
PPL ELECTRIC UTILITIES CORPORATION**

---

Kimberly A. Klock (ID #89716)  
Michael J. Shafer (ID #205681)  
PPL Services Corporation  
Two North Ninth Street  
Allentown, PA 18101  
Voice: 610-774-5696  
Fax: 610-774-4102  
E-mail: [kklock@pplweb.com](mailto:kklock@pplweb.com)  
E-mail: [mjshafer@pplweb.com](mailto:mjshafer@pplweb.com)

Date: February 8, 2023

Counsel for PPL Electric Utilities Corporation

## TABLE OF CONTENTS

	<b>Page</b>
I. BACKGROUND .....	1
II. COMMENTS .....	1
A. INTRODUCTION .....	2
B. UPDATING TERMS AND CONCEPTS.....	4
C. EXPLORING APPROACHES TO ENSURING CYBERSECURITY FITNESS IN PUBLIC UTILITIES.....	4
D. IMPROVING THE SELF-CERTIFICATION FORM (SCF) PROCESS .....	8
E. UPDATING CYBERATTACK REPORTING REGULATIONS .....	8
F. MERGING THE SELF-CERTIFICATION AND CYBERATTACK REPORTING REGULATIONS.....	9
G. COST-BENEFIT ANALYSIS.....	10
H. ELIMINATING REGULATORY DUPLICATION AND OVERLAP .....	10
I. OTHER MATTERS.....	11
III. CONCLUSION.....	12

## **I. BACKGROUND**

On November 10, 2022, the Pennsylvania Public Utility Commission (“Commission”) entered an Advance Notice of Proposed Rulemaking Order (“ANOPR”) at the instant docket. In the ANOPR, the Commission observed that it currently has cyberattack regulations at 52 Pa. Code §§ 57.11, 59.11, 61.11, and 65.2 for electric, natural gas, steam, and water utilities, respectively, and self-certification regulations at 52 Pa. Code §§ 101.1-101.7 and 61.45, the latter of which applies to steam utilities. Through the ANOPR, the Commission has 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. Attached to the ANOPR as Appendix A are 15 topics on which the Commission seeks comments.

PPL Electric Utilities Corporation (“PPL Electric”) appreciates the opportunity to provide comments to the Commission regarding the issues identified in the ANOPR and hereby states the following:

## **II. COMMENTS**

As a preliminary matter, PPL Electric supports the Comments filed by the Energy Association of Pennsylvania (“EAP”) on behalf of its members, which includes PPL Electric. PPL Electric offers its own independent comments to direct attention to matters that are particularly important to PPL Electric.

## **A. INTRODUCTION**

### **1. 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**

Cybersecurity is critical to the safe and reliable operation of PPL Electric's electric facilities and systems. As such, PPL Electric takes its role in protecting its facilities, systems, and customer information from cyberattacks very seriously and devotes substantial time and resources to protecting against them. At the parent level, PPL Corporation's ("PPL") cybersecurity strategy is a regular topic of discussion at board of directors meetings. PPL's company-wide strategy for managing cyber-related risks is risk-based and, where appropriate, integrated within PPL's enterprise risk management processes.

PPL's cybersecurity strategy is aligned with and informed by the following:

- Current and emerging cybersecurity threats.
- Industry best practices, control frameworks and industry standards.
- Emerging security technologies and capabilities.
- National Institute of Standards and Technology Cybersecurity Framework.
- North American Electric Reliability Corporation Critical Infrastructure Protection mandatory standards.
- Government and law enforcement security intelligence sharing.
- Industry collaboration and information sharing.

Furthermore, PPL's cybersecurity team strategy includes:

- Actively monitoring company systems.
- Regularly reviewing policies, compliance, regulations and best practices.
- Conducting assessments and penetration testing.

- Conducting incident response exercises and internal ethical phishing campaigns.
- Providing training and communication across the organization to strengthen and foster a culture of security.
- Corporate governance in the form of a Corporate Security Council that meets quarterly to review and understand cybersecurity and physical security risks, and direct actions to improve PPL's security posture.
- Routinely participating in industry-wide programs to further information sharing, intelligence gathering, and unity of effort in responding to potential or actual attacks.
- Numerous other investments that span people, processes and technology.

In addition to the Commission's current regulations, stringent cybersecurity requirements applicable to certain electric utilities exist, which include disclosure and reporting requirements. For example, certain utilities are currently subject to the cybersecurity reporting requirements of the North American Electric Reliability Corporation ("NERC"), the Federal Energy Regulatory Commission ("FERC"), the Transportation Security Administration ("TSA"), the U.S. Department of Energy ("DOE"), and other federal agencies.

PPL Electric believes that the Commission should take those existing requirements into account before layering on additional, redundant, or even perhaps conflicting requirements, which will complicate public utilities' responses to cyberattacks and increase the public utilities' expenses. Notwithstanding, as set forth in the following sections, the Commission's regulations could benefit from some clarification.

## **B. UPDATING TERMS AND CONCEPTS**

### **1. 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**

PPL Electric recommends that the Commission consider the many state and federal regulatory cybersecurity requirements that electric utilities already are subjected to and required to comply with, many of which have unique disclosure and reporting requirements and other mandates. Indeed, as noted previously, certain electric utilities are subject to cybersecurity reporting requirements of, among other entities, NERC, FERC, TSA, and DOE. Electric utilities would benefit from consistency in the notification requirements, reporting requirements, and applicable definitions to which they are subjected. By avoiding contradictory or duplicative requirements, electric utilities can better focus on and devote scarce cyber resources to protecting critical systems, assets and information. Such consistency across the requirements will bolster the protection of critical systems, assets, and information, which is imperative for national security and the safety and protection of employees, customers, and the general public.

## **C. EXPLORING APPROACHES TO ENSURING CYBERSECURITY FITNESS IN PUBLIC UTILITIES**

### **1. Relative Merits and Weaknesses of Each of the Approaches Within the Heading “Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities”**

In its ANOPR, the Commission sets forth “five potential regulatory approaches to ensure that public utilities have adequate cybersecurity plans in place to respond to cyber threats.”

ANOPR, p. 12. Those approaches are:

1. “Similar to the 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 to report annually to the PUC that such plans and/or programs exist and are updated and tested annually.” ANOPR, p. 12.

2. “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.” *Id.*
3. “Require a public utility to provide a third-party expert certification that the public utility has a plan, a program, or both, in place that comply 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.” *Id.*
4. “Integrate an onsite review of cybersecurity measures, plans, and programs into the PUC’s public utility management audit process and examine cybersecurity measures, plans, and programs in place as a part of the management audit function.” *Id.*, p. 13.
5. “Require a public 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.” *Id.*

PPL Electric supports Approaches 1 and 2. These approaches ensure that utilities are reviewing, evaluating, testing, and updating their plans and programs annually, all without requiring that sensitive and confidential cybersecurity plan information be transferred outside of the utility<sup>1</sup> and are not resource-intensive to complete, nor will they result in duplicative reporting or redundancies with the applicable Commission, federal, and/or industry rules and requirements.

---

<sup>1</sup> Transferring this information outside of the utility, even to the Commission, could create unnecessary risk of public disclosure of this sensitive information.

Conversely, Approaches 3, 4, and 5 are not supported by PPL Electric. Although Approach 3 could provide some further assurance to the Commission, such third-party expert certification would be costly. Moreover, any sharing of such information with a third party would add risk that the cybersecurity plan information could be compromised. Also, PPL Electric believes that establishing and validating qualified third parties to perform annual certifications would not only be costly, but would divert precious and scarce cyber resources away from implementing and maintaining cyber protections, to preparing, responding, and reporting to third parties. Additionally, Approach 4's audit process would be resource and time-intensive and at least somewhat duplicative with the Commission's management audits of public utilities. Approach 4 would take substantial time and effort to ensure that all standards for protection of confidential information are satisfied in order for the Commission to perform such an on-site review. Lastly, Approach 5 would be resource and time-intensive as well. And, although it may enable the Commission to have an added layer of oversight on cybersecurity, PPL Electric believes that housing all of the public utilities' sensitive and confidential cybersecurity plans in a single location outside of the utility's control would be an unnecessary risk. As noted previously, the Commission can already review these plans and provide feedback during its management audit process.

**2. Approaches Taken by Other State Public Utility Commissions to Address Public Utilities' Cybersecurity Fitness, and Evaluating Their Respective Costs and Benefits**

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

**3. Whether Changes to the Cybersecurity Aspect of 52 Pa. Code § 101.3 Would Impact the Physical Security, Emergency Response, and/or Business Continuity Aspects of the Rule and/or Chapter 101 Generally**

PPL Electric believes that it is premature to state conclusively whether changes to the cybersecurity aspect of Section 101.3 of the Commission's regulations would affect the physical security, emergency response, and/or business continuity aspects of that regulation or other

regulations in Chapter 101. The actual proposed changes would be needed to complete that evaluation.

Nevertheless, PPL Electric observes that cybersecurity, physical security, emergency response, and business continuity are inextricably connected in today's environment. For example, several events have both cyber and physical security impacts, such as compromised business emails, insider threats or employee misconduct involving a cyber asset, and theft or vandalism of a cyber asset. Therefore, it is essential that the impact on physical security, emergency response, and business continuity be considered when making any changes to the Commission's cybersecurity regulations.

PPL Electric believes the Commission should also clarify the reporting requirements to reflect the fact that events often involve both cyber and physical security impacts, including, but not limited to, allowing public utilities to submit a single report to the Commission's Director of Emergency Preparedness for an event affecting both cyber and physical security, rather than requiring the submission of multiple reports.

**4. Whether the Self-Certification Regulations Should Be Applied to Additional Types of Entities that Are Subject to the Commission's Supervision**

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

**5. Whether There Are Public Utility Types that Should Be Wholly or Partially Exempt from the Self-Certification, Based on Easing the Regulatory Burden on Small Businesses, or for Other Reasons**

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

## **D. IMPROVING THE SELF-CERTIFICATION FORM (SCF) PROCESS**

### **1. Ways to Streamline and Otherwise Improve the Filing, Handling, and Storage of SCFs**

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

### **2. 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 Commission Staff**

As stated in Section C. 1, the Commission could consider adding to the self-certification form an option for public utilities to report that they have a plan, a program, or both, that complies with an appropriate federal or industry standard. This approach would provide more information regarding the substantiveness of a utility's program without requiring the utility provide the sensitive and confidential details of its cybersecurity plan.

## **E. UPDATING CYBERATTACK REPORTING REGULATIONS**

### **1. Potential Ways to Revise the Reporting Criteria in the Commission's Existing Regulations, Including the Potential Addition of New Requirements for Reporting Incidents Involving IT**

While PPL Electric does not think additional reporting requirements are needed, the existing regulations could be improved by clarifying under what conditions reporting is required as noted in Section E.2 below, how utilities should report confirmed incidents involving IT, and specifically to whom at the Commission public utilities should report confirmed incidents involving IT. The Commission should also consider that many incidents involve both IT and physical security, as noted above. Therefore, an incident's scope is not always immediately clear. As a result, PPL Electric believes that reportable cyber and physical incidents should be reported to the Commission's Director of Emergency Preparedness for further distribution to other impacted parties, if necessary.

**2. Whether the Commission Should Continue the \$50,000 Reporting Threshold**

PPL Electric does not believe that the Commission should continue the \$50,000 reporting threshold. As noted in the ANOPR, the \$50,000 criterion is ambiguous. *See* ANOPR, p. 17. The economic impact of cyberattacks is difficult to quantify, especially during the early stages of incident resolution. Accordingly, the Commission should remove the \$50,000 reporting threshold from its regulations. In its place, PPL Electric maintains that reporting triggers for confirmed cybersecurity incidents should be based on the interruption of the utility's service to customers.

**F. MERGING THE SELF-CERTIFICATION AND CYBERATTACK REPORTING REGULATIONS**

**1. 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**

By merging the self-certification and cyber incident reporting regulations into a single chapter of the Commission's regulations, PPL Electric believes that the Commission could improve uniformity, simplify its regulations, and eliminate inconsistencies. Additionally, the process for merging the self-certification and cyber incident reporting regulations should consider how cybersecurity, physical security, and emergency preparedness are related and should retain the components of existing regulations that apply to the types of incidents in Section 57.11, with the exception of the \$50,000 reporting threshold. This will ensure that confirmed incidents of both cyber and physical nature, for example, can be reported in one single report (rather than having a separate and distinct process for reporting the incident as it relates to cyber security and as it relates to physical security).

## **G. COST-BENEFIT ANALYSIS**

### **1. How to Best Justify Revisions to the Existing Regulations under the Regulatory Review Act Standards, Particularly How the Costs and Benefits Associated with the Commission’s Existing Regulations, and Any Revisions Thereto, Can Be Objectively Quantified and Evaluated**

PPL Electric recognizes that the Commission’s potential revisions to the cybersecurity regulations will need to be evaluated under the Regulatory Review Act’s standards on a cost-benefit basis. Although it is premature to quantify those costs and benefits, given that the actual proposed changes to the Commission’s regulations are unknown, PPL Electric believes that potential costs could include the costs to implement any required program or reporting changes, such as legal fees, testing costs, engagement of costly third-party services, and on-going reviewing costs. Additionally, benefits could include a greater understanding of incidents and the avoidance of costs related to duplicative reporting and requirements.

## **H. ELIMINATING REGULATORY DUPLICATION AND OVERLAP**

### **1. Potential for Conflict, Overlap, Redundancy, or Other Bases Warranting Review in the Interplay Between the Commission’s Cybersecurity Regulations (and Revisions Thereto) and Federal Initiatives, Including but Not Limited to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA)**

To the extent the Commission believes there may be conflicts between requirements, it could allow utilities the option to self-certify that their plans and programs comply with federal and/or industry standards. This would avoid any issues concerning the interplay between the Commission’s regulations and federal initiatives, including CIRCA. Specifically, Section 101.6(d) of the Commission’s regulations states that “[a] utility that has developed and maintained a cyber security, physical security, emergency response or business continuity plan under the directive of another state or Federal entity that meets the requirements of § 101.3 (relating to plan requirements) may utilize that plan for compliance with this subpart, upon the condition that a

Commission representative be permitted to review the cyber security, physical security, emergency response or business continuity plan.” 52 Pa. Code § 101.6(d). By retaining this procedure, public utilities will be able to avoid any potential conflicts with how CIRCIA, which still needs to go through the rulemaking process, is ultimately implemented. This concern is particularly important to entities like PPL Electric that have affiliates operating in other jurisdictions and that have many other reporting requirements and reviews, both internal and external (e.g., annual internal risk-based audits, NERC requirements and audits, peer reviews). Thus, allowing utilities the option to self-certify that their plans and programs comply with federal and/or industry standards, would avoid redundant requirements and, ultimately, reduce costs for customers.

**I. OTHER MATTERS**

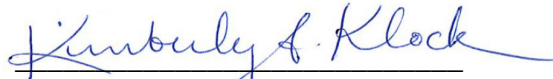
**1. Any Additional Considerations that Parties May Wish to Raise at This Time Relating to Commission Oversight and Regulation of Public Utilities and Licensed Entities as It Relates to Their Cybersecurity Fitness**

PPL Electric has no further Comments.

### III. CONCLUSION

PPL Electric appreciates the opportunity to provide these Comments and respectfully requests that the Commission take these Comments into consideration when developing any proposed update to its cybersecurity regulations.

Respectfully submitted,



Kimberly A. Klock (ID #89716)

Michael J. Shafer (ID #205681)

PPL Services Corporation

Two North Ninth Street

Allentown, PA 18101

Voice: 610-774-5696

Fax: 610-774-4102

E-mail: [kklock@pplweb.com](mailto:kklock@pplweb.com)

E-mail: [mjshafer@pplweb.com](mailto:mjshafer@pplweb.com)

Date: February 8, 2023

Counsel for PPL Electric Utilities Corporation