Lindsay Baxter
Manager, Regulatory and Clean Energy Strategy
lbaxter@duqlight.com
(412) 393-6224

February 8, 2023

VIA ELECTRONIC FILING

Ms. Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
2nd Floor, Room-N201
400 North Street
Harrisburg, PA 17120

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 please find Duquesne Light Company's Comments for filing in the above referenced proceeding.

If you have any questions regarding the information contained in this filing, please feel free to contact me.

Sincerely,

Lindsay A. Baxter
Manager, Regulatory and Clean Energy Strategy

Enclosure
cc (w/ enc):
Colin Scott, Law Bureau, colinscott@pa.gov
Chris Van de Verg, Law Bureau, cvandeverg@pa.gov
Daniel Searfoorce, Bureau of Technical Utilities Services, dsearfoorc@pa.gov
Michael Holko, Office of Cybersecurity Compliance and Oversight, miholko@pa.gov
Karen Thorne, Law Bureau, kathorne@pa.gov

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

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

COMMENTS OF
DUQUESNE LIGHT COMPANY

I. INTRODUCTION

On November 10, 2022, the Pennsylvania Public Utility Commission ("Commission" or "PUC") entered an Advanced Notice of Proposed Rulemaking Order ("ANOPR" or "Order") seeking comments regarding the sufficiency of, and potential revisions to, the regulations at 52 Pa. Code §§ 57.11 (relating to accidents for electricity public utilities), 59.11 (relating to accidents for gas public utilities), 61.11 (relating to accidents for steam utilities), 65.2 (relating to accidents for water public utilities), 101.1-101.7 (relating to public utility preparedness through self-certification) and 61.45 (relating to security planning and emergency contact list for steam utilities). Interested parties were invited to file written comments within 60 days after the date of publication in the *Pennsylvania Bulletin*, which occurred December 10, 2022. Accordingly, Duquesne Light Company ("Duquesne Light" or "Company") submits these comments for the Commission's consideration.

II. BACKGROUND

In 2005, the Commission worked with Pennsylvania's Office of Homeland Security to coordinate security efforts. From this collaboration, the Commission promulgated regulations

developing a security self-certification process for all jurisdictional utilities.[1] These regulations require "all jurisdictional utilities to develop and maintain written physical, cyber security, emergency response and business continuity plans to protect the Commonwealth's infrastructure and ensure safe, continuous and reliable utility service."[2] Each utility must submit an annual Self-Certification Form ("Form") that asserts the utility has a cybersecurity plan in place.[3]

Additionally, in 2011, the Commission promulgated regulations regarding cyber-attack reporting.[4] These regulations were expanded to include "an occurrence of an unusual nature that is a physical or cyber-attack, including attempts against cyber security measures… … that causes an interruption of service or over $50,000 damages, or both."[5]

Through the ANOPR, the Commission is seeking feedback as to whether the Form and cyber-attack 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."[6]

Duquesne Light is a public utility as the term is defined under Section 102 of the Public Utility Code, 66 Pa.C.S. § 102, and is certificated by the Commission to provide electric distribution service in portions of Allegheny and Beaver Counties in Pennsylvania. Duquesne Light provides electric service to nearly 610,000 customers in and around the City of Pittsburgh. As an electric distribution company ("EDC") subject to the provisions of these regulations, Duquesne Light is an interested stakeholder in this proceeding and files these responsive comments to the ANOPR.

---

[1] Revised Final Rulemaking Order, *Rulemaking re Public Utility Security Planning and Readiness*, Docket No. L-00040166 (entered Mar. 10, 2005).
[2] *Id*. at 1.
[3] 52 Pa. Code §§ 101.1-101.7 (relating to public utility preparedness through self-certification).
[4] Final Rulemaking Order, *Proposed Rulemaking for Revision of 52 Pa. Code Chapters 57, 59, 65 and 67 Pertaining to Utilities' Service Outage Response and Restoration Practices*, Docket No. L-2009-2104274 (entered Sept. 23, 2011).
[5] *See* 52 Pa. Code §§ 57.11(b)(4), 59.11(b)(5) and 65.2(b)(4).
[6] ANOPR at 2.

III. COMMENTS

A. Introduction

The cyber industry is constantly changing, with increased vigilance needed by all to ensure both cyber and physical safety. Duquesne Light works to maintain the highest of standards in cybersecurity. Its cybersecurity program, under the leadership of a Chief Information Security Officer, protects, detects, responds to, and recovers from cyber attacks to safeguard the people, processes, and technology required to deliver reliable service. The Company has deployed capabilities to rapidly detect, respond, contain, and recover from threats, and measures key information security processes by collecting and analyzing data and continuously improving cybersecurity processes. Duquesne Light's strategies align with and adhere to national standards and the Company partners with U.S. Government, federal and state law enforcement security agencies, and industry peers for threat and information sharing.

The Company appreciates the Commission's efforts to ensure regulations and processes are updated as needed to coincide with an evolving industry and increasing cybersecurity risks. However, the Company also encourages the Commission to weigh the risks of potential exposure of sensitive information with any potential benefits of new regulations. The Company looks forward to working with the Commission and stakeholders throughout this process to ensure the cybersecurity needs of the utilities and their customers are met.

B. Updating Terms and Concepts

The Commission solicits feedback on the need for updating terms and concepts used in the regulations. The Commission notes that definitions and terms have evolved since 2005 when

the self-certification regulations were promulgated.[7] Duquesne Light agrees that certain terms may need to be updated to reflect current times and practices more fully. To the extent possible, the Company recommends the PUC use definitions in existing statute or regulation, such as the "Breach of Personal Information Notification Act."[8] Duquesne Light does not offer specific terms or definitions at this time, but looks forward to the opportunity to review and comment on the recommended definitions of other commenters, and/or those proposed by the Commission, should it move forward with a Notice of Proposed Rulemaking.

C. Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities

i. Potential Regulatory Approaches

The Commission outlined in the ANOPR five potential regulatory approaches that it believes could ensure utility cybersecurity plans that respond to cyber threats:

- 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.
- 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.
- 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.
- 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.
- 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

[7] *Id.*at 8-9.
[8] *See* 73 Pa. C.S. § 43.

> on the adequacy of such plans and programs and, where deficiencies exist, require conformance with regulatory standards.[9]

Duquesne Light supports the first bullet regarding submission of a Form wherein a utility self-certifies that it has a plan, program or both that complies with the PUC's regulations. The Company finds that the current practice of self-certification through the existing Form is appropriate and adequate in providing certainty to the Commission that utilities are providing the necessary cybersecurity, emergency response, business continuity, and physical security plans without unnecessarily exposing confidential information or risking the physical or cyber safety of the utilities, their employees, and the ratepayers of the Commonwealth. The Company does not propose any changes to the existing Form at this time.

Regarding the second bullet, while the Company supports utility compliance with Federal and industry standards, it opposes certification of compliance and/or provision of detailed information regarding Federal standards to the Commission. Many Federal standards focus on transmission and critical infrastructure assets and are not appropriate for adoption at the distribution level. Additionally, not all standards are applicable across all utility types or even utility sizes (e.g., large versus small utilities) and, as such, may make inclusion of them in a Form difficult if the aim is uniformity. Compliance with these standards is already reviewed by other Federal agencies and entities, such as the North American Electric Reliability Corporation ("NERC"). Any additional benefit resulting from also filing such a self-certification with the Commission is unclear and may not outweigh the potential risks.

The Company strongly opposes the final three approaches outlined by the Commission. They open sensitive cyber information to other parties, creating additional confidentiality and security risks. The Company asserts that any benefits purportedly tied to any of the three options

[9] ANOPR at 12-13.

certainly do not outweigh the risks of providing such information, counter to the intent of these regulations. Should the Commission pursue any of these options in a future Notice of Proposed Rulemaking, it should clearly define how this information fits within the Commission's jurisdictional oversight, to whom information will be provided, what information is to be included in any plans or programs, how that information will be maintained confidentially and securely, and the benefits and goals of the proposed approach.

ii. Approaches in Other States

The Commission seeks comments on any supportable cybersecurity approaches taken by other states or jurisdictions.[10] At this time, the Company does not have enough familiarity with the approaches of other states to respond to this question.

iii. Impacts of Changes to 52 Pa. Code § 101.3

The Commission requests feedback on how changes to cybersecurity plan requirements in this section may impact physical security, emergency response, and/or business continuity aspects of the regulation.[11] The Company recognizes the interconnectedness of these plans; however, it is difficult to assess impacts in advance of reviewing specific proposed changes.

iv. Other Entities' Self-Certification

In its ANOPR, the Commission requests feedback on whether the self-certification regulations should apply to additional types of entities under the PUC's supervision.[12] The

[10] *Id.* at 13.
[11] *Ibid.*
[12] *Ibid.*

Company suggests that those entities with access to customer information be required to ensure such information is kept confidential and prove themselves fit technically to ensure cybersecurity is maintained. For example, it may be appropriate to require electric generation suppliers ("EGSs") to submit the Form as they have access to customer data and sensitive information through electronic data interchange ("EDI") and other avenues. Additionally, when Federal Energy Regulatory Commission ("FERC") Order 2222[13] is implemented, it may be appropriate to require distributed energy resource aggregators to self-certify, as well.

v. Self-Certification Exemptions

The Commission requests comments regarding Form exemptions for certain public utility types, for example, small businesses.[14] The Company cannot speak to the level of sophistication of smaller utilities, but recognizes there may be variations in the application of the self-certification regulations based on size, business type, operation of first-tier critical infrastructure, etc. As noted in the previous section of these Comments, data interchanges processes, the conveyance and storage of sensitive customer information, and the maintenance of critical facilities may necessitate the need for self-certification regardless of business size. The Company asserts that flexibility may be important, while still recognizing the need to ensure information is maintained safely.

[13] *Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators*, 172 FERC ¶ 61,247 (2020) ("Order 2222").
[14] ANOPR at 14.

D. Improving the Self-Certification Form Process

Regarding the Form's process, the Commission seeks feedback on streamlining the filing, handling and storage of the Forms, as wells as how to "better calibrate the benefits of the existing regulations against the burdens they place on regulated entities, especially smaller utilities, and on PUC staff."[15] The Company is not advocating for changes to the Form's content at this time. However, as noted herein, flexibility regarding the Form's applicability to other entities (e.g., EGSs, smaller utilities) is advisable and, as such, may impact the Commission's handling of information. Duquesne Light does not have specific comments regarding the process other than again advocating that all information be maintained confidentially, with limited access. Should the PUC move forward with changes to the Form, changes to Commission procedures may be necessary to ensure sensitive information is not inadvertently released or provided beyond those who need to see it to perform their job duties.

E. Updating Cyber Attack Reporting Regulations – Revising Reporting Criteria and $50,000 Reporting Threshold

The Commission requests comments on ways to revise the reporting criteria for cyber attacks, including potential new requirements for IT-related incidents.[16] The current regulations require the reporting of a physical or cyber attack that causes over $50,000 in damages.[17] The Company highlights the interconnectedness of IT and operating systems and believes it is most appropriate to focus on impacts to operations or data security (both customer and employee) in setting the threshold for reporting cyber attacks. Reporting is likely necessary when there is a

[15] *Id.* at 15-16.
[16] *Id*. at 16.
[17] *See* 52 Pa. Code § 57.11(b)(4).

breach of the confidentiality or integrity of the utility's system or if there is malicious exposure of data protected by Pennsylvania statutes and regulations. Reportable incidents could potentially include any attack or incident that causes a material impact to operational control or visibility, or sensitive data confidentiality, integrity or availability.

F. Merging the Self-Certification and Cyber Attack Reporting Regulations

In reviewing the regulations regarding self-certification and cyber attack reporting, the Commission seeks feedback on whether to merge these two requirements into a single chapter of the Code.[18] The Company cannot assess the benefits or detriments to merging the regulations without proposed regulatory changes.

G. Cost-Benefit Analysis

The Commission requests feedback on justifying revisions to the regulations, including costs-benefit impacts of any changes.[19] The Company believes this request is premature as it cannot assess cost-benefit impacts prior to reviewing specific proposed regulatory changes.

H. Eliminating Regulatory Duplication and Overlap

In its ANOPR, the Commission discusses how its regulations may be affected by other initiatives, such as the Federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").[20] The Company supports steps to reduce redundancies and conflicts in cyber incident reporting. While a central hub for reporting may make sense, reporting changes may be

[18] ANOPR at 18.
[19] *Id.* at 19.
[20] *Id.* at 20-21.

better addressed in a Notice of Proposed Rulemaking when clearly articulated proposed regulatory changes are available to help inform what reporting is to be performed.

IV. CONCLUSION

Duquesne Light is supportive of efforts to ensure cybersecurity is maintained and utility customers protected. The Company urges the Commission to carefully consider the benefits of any future proposed regulations and weigh them against any potential confidentiality or security risks. Duquesne Light supports flexibility in keeping up with the ever-changing cyber landscape and appreciates the Commission's consideration of these comments.

Respectfully submitted,

Lindsay A. Baxter
Manager, Regulatory and Clean Energy Strategy
Duquesne Light Company
411 Seventh Avenue, Mail Drop 15-7
Pittsburgh, PA 15219
lbaxter@duqlight.com
Tel. (412) 393-6224

DATE: February 8, 2023