Lindsay Baxter
Senior Manager, Energy Policy and Public Affairs
lbaxter@duqlight.com
412-393-6224

July 16, 2025

VIA ELECTRONIC FILING

Matthew Homsher, 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 Homsher

Enclosed for filing please find Duquesne Light Company's Comments 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
Senior Manager, Energy Policy and Public Affairs

Enclosure

cc:
Colin Scott, colinscott@pa.gov
Chris Van de Verg, cvandeverg@pa.gov
Daniel Searfoorce, dsearfoorc@pa.gov
Michael Holko, miholko@pa.gov
Karen Thorne, 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

At the November 10, 2022 Public Meeting, the Pennsylvania Public Utility Commission ("PUC" or "Commission") initiated a review of its cybersecurity self-certification requirements by issuing an Advanced Notice of Proposed Rulemaking ("ANOPR") for public comment. Nineteen interested parties, including Duquesne Light Company ("Duquesne Light" or "Company"), filed comments. On April 25, 2025, the Commission adopted a Supplemental ANOPR on this topic. In summary, the Supplemental ANOPR presents a staff working proposal for stakeholder input. The staff proposal recommends maintaining self-certification and reporting related to *physical* security and establishing a new Chapter 103 related to cybersecurity assessments, programs, standards and plans. The staff proposal also recommends a new Chapter 104 related to cybersecurity incident reporting.

The Supplemental ANOPR Order requests interested stakeholder comment on thirteen specific questions. Public Comment is due sixty days following publication in the *Pennsylvania Bulletin.* Notice of the public comment period was published May 17, 2025 (*55 Pa.B. 3379)*, which establishes a due date for comments of July 16, 2025. Duquesne Light hereby submits these comments for consideration.

II. BACKGROUND

Duquesne Light Company 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 approximately 605,000 customers in and around the City of Pittsburgh. As an electric distribution company ("EDC"), the Company is subject to the Commission's cybersecurity self-certification and reporting requirements.

III. COMMENTS

Cybersecurity represents one of the top risks facing the utility sector today, with the potential for exposure of customer data, as well as potentially cascading impacts on reliability. Before turning to the specific questions posed by the ANOPR, Duquesne Light emphasizes two points that frame its comments:

1) Cybersecurity regulations adopted by the PUC should only apply to assets not already subject to federal cybersecurity protections. The Commission should clearly recognize that certain electric utilities within Pennsylvania own, operate, and maintain transmission facilities already under the regulatory jurisdiction of the Federal Energy Regulatory Commission ("FERC"). These transmission facilities and the associated cyber systems are part of the Bulk Electric System ("BES") and subject to existing reliability and security expectations established by the North American Electric Reliability Corporation ("NERC") at FERC's direction. The NERC Reliability Standards applicable to the BES include FERC-approved mandatory requirements that can result in fines and penalties for non-compliance of $1,000,000 per day per violation. Any cybersecurity regulations,

policies, or guidance adopted by the PUC should clearly state that they apply only to EDC facilities not already covered by the NERC Critical Infrastructure Protection ("CIP") Reliability Standards.[1]

BES Cyber Systems and their associated BES Cyber Assets must be operated and maintained in accordance with the FERC-approved NERC CIP Reliability Standards. These Standards include cybersecurity expectations and requirements applicable to areas including personnel, access management (physical and electronic), network and cyber asset security protections, cyber incident response, cyber asset recovery, and incident reporting. There is no additional benefit to creating overlapping cybersecurity requirements for these BES assets; rather doing so would only create additional burden and complexity for utilities and regulators.

For each of Duquesne Light's responses below, it should be assumed the Company is responding with the understanding that state regulations will only apply to assets not already under the regulatory jurisdiction of FERC as determined by the NERC CIP Reliability Standards.

2) Duquesne Light commends the Commission for recognizing the existing resources, guidelines, and regulations on this topic produced by diverse federal agencies and industry organizations and urges the PUC to avoid duplicating efforts. The PUC should

[1] The NERC CIP Reliability Standards include a required process to establish a clear scope of the cyber systems covered by FERC regulatory jurisdiction. NERC Reliability Standard CIP-002-5.1a details the steps required of an electric utility to identify and categorize BES Cyber Systems included within the scope of the NERC CIP Reliability Standards as stated in the purpose of the Standard: *"To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES."*

avoid "recreating the wheel" and instead focus on ensuring utilities are aligning with existing requirements and best practices.

With this framing in mind, Duquesne Light offers responses to the questions posed in Appendix A: Topics for Comment, below.

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?

   As stated in its initial framing, the Company only supports additional PUC-imposed requirements that apply to facilities *not already covered by FERC regulatory jurisdiction and the NERC Reliability Standards*. It would be appropriate and beneficial for the Commission to require jurisdictional utilities to maintain cybersecurity programs and plans that conform to accepted standards and frameworks, such as the NIST Cybersecurity Framework or the Department of Energy/National Association of Regulated Utility Commissioners ("NARUC") Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources.[2] The Company cautions the Commission to avoid being overly prescriptive, though, and to allow a degree of flexibility. Should the Commission move forward with such requirements, Duquesne Light recommends requiring utilities to align around a common framework, without requiring a specific publication number.

[2] NIST Cybersecurity Framework at www.nist.gov/cyberframework; NARUC Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources at www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/.

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?

Duquesne Light contends that certain baseline requirements should apply to any utility to ensure adequate safeguarding of customer data and to protect reliability. However, the Company agrees that it is appropriate to exercise flexibility based on the size and individual characteristics of a utility. The PUC proposes organizing utilities into five classes based on size and risk profile, as follows:

- Class 1 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility serving 100,000 or more customers.
- Class 2 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility serving at least 3,300 customers but less than 100,000 customers.
- Class 3 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility serving less than 3,300 customers.
- Class 4 utility—Any common carrier that (1) electronically collects and stores personal information; (2) uses IT; or (3) uses OT.
- Class 5 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility that does not (1) electronically collect or store personal information; (2) use IT; and (3) use OT.

A tiered approach ensures that cybersecurity obligations are proportional to a utility's operational scale and criticality. Criteria for classification should be

expanded beyond just a simple customer count, to also include metrics such as type and complexity of infrastructure; interconnection with other critical systems; and/or financial and technical resources. Rather than a static threshold, the Commission could consider a matrixed approach that evaluates a number of metrics to determine the appropriate tier.

Additionally, the Commission can provide flexibility by avoiding being overly prescriptive in how utilities achieve compliance. The PUC should set the expectation for cybersecurity protections but allow flexibility in how each organization complies.

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

Yes, the Commission should allow for a waiver process that is transparent and predictable. The PUC should outline waiver criteria such as:

- Demonstrated cybersecurity maturity or third-party certification
- Use of alternative but equivalent or superior frameworks (ex. ISO 27001)
- Risk assessments showing minimal exposure
- Documented incident response and recovery capabilities

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. Doing so encourages innovation and incentivizes utilities to adopt industry-leading best practices. The Commission should allow such waivers if the utility can:

- Map its framework to NIST Cybersecurity Framework standards
- Demonstrate equivalent or better risk mitigation
- Provide third-party validation or audit results

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?

Yes, the Commission can provide this flexibility without compromising security. As cybersecurity practices and standards evolve, there may be provisions that do not apply to smaller utilities, or for which compliance is impractical. The Company cautions, though, that waivers from certain standards and frameworks should not be granted based on size alone. Smaller utilities must be able to show that certain controls are not relevant or feasible, and that their risk exposure is low.

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

The Commission should endeavor to craft regulations that are "evergreen," to the extent possible. However, recognizing the rapidly evolving nature of cybersecurity, the Company recommends the Commission establish a working group of utility stakeholders, including cybersecurity experts, to periodically review any updates to standards and frameworks and, if necessary, recommend updates to PUC practices and/or regulations.

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

The Company recommends the PUC maintain its current practice of requiring an annual self-certification compliance filing. This approach balances the significance of this subject matter, by requiring the approval of an officer, subject to the penalties of 19 Pa. C.S. § 4904 (relating to unsworn falsification to authorities), with limiting the administrative burden and cost to the utility and the Commission.

To the extent the Commission wishes to complete a more comprehensive review of compliance, the Company notes that cybersecurity plans and incident response documentation can be subject to review during a PUC Management Audit.

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

The PUC has existing authority under Chapter 5 of the Public Utility Code to supervise and regulate all public utilities doing business within the Commonwealth. *See, e.g.,* 66 Pa.C.S. §501(b). The Company further submits that the cybersecurity measures at issue in this proceeding are consistent with reasonable service provisions of the Public Utility Code. *See*, 66 Pa.C.S. §1501. The Company does not believe additional enforcement mechanisms are required in the proposed Chapter 103 and 104.

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)?

Yes, an annual certification by a public utility that it adheres (or does not adhere) to a specific cybersecurity standard could reasonably be considered Confidential Security Information ("CSI") under Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act, 35 P.S. §§ 2141.1–2141.6 (CSI Act), depending on the content and context of the certification. The CSI Act defines "confidential security information" as information that, if disclosed, could compromise security against sabotage, criminal, or terrorist acts, and whose nondisclosure is necessary to protect life,

safety, public property, or utility infrastructure. The annual certification, particularly if it discloses non-adherence, could lead to a serious security concern if publicly disclosed.

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?

   The Commission should maintain a dedicated, encrypted electronic filing system that:

   - Requires multi-factor authentication for access
   - Supports role-based access control with least privilege access control to limit who can view CSI
   - Logs all access and submission activity for audit purposes
   - Enforces labeling and data segregation
   - Enforces encryption at rest and in transit
   - Follows strict protocols for internal sharing and storage of backups
   - Sends a secure acknowledgment receipt to the utility
   - Confirms that the filing has been properly classified and stored
   - Conducts internal audits to ensure internal compliance and transparently share those reports with the utility
   - Provides guidance documents to utilities on secure filing practices

The Company reiterates the point that a self-certification form similar to that currently filed may be most appropriate to avoid the disclosure of potentially sensitive information. Utilities employ robust security measures; it is unclear if the state government system maintains the same protections. The Company contends that the PUC could be a target for bad actors seeking to access utility data. To limit this risk, the Commission should avoid including highly sensitive information on the annual certification.

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?

   Yes, these purposes are largely similar. The Commission should avoid duplicating any requirements that already exist at the federal level.

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).

   For the areas a. through d., Duquesne Light believes no additional involvement by the PUC is necessary. Resources like NERC's Electric Information Sharing and Analysis Center ("E-ISAC"), Infragard, the Federal Bureau of Investigation ("FBI"), and Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency already effectively provide this information-sharing function. If anything, the PUC should amplify these existing avenues to regulated entities.

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).

The PUC can support federal cybersecurity efforts by fostering collaboration with agencies like DHS and FBI, promoting best practices, and encouraging utilities to share anonymized incident data for research. Additionally, it should engage with software and equipment vendors to address vulnerabilities and align state regulations with evolving federal standards.

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?

The Company reiterates its response to item e.

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

Certain types of public utilities could be considered for exemption from cyber incident reporting if they pose minimal risk to critical infrastructure, have limited digital exposure, or serve a very small customer base. However, any exemption should be carefully evaluated to ensure it does not create blind spots in the state's overall cybersecurity posture, especially as even small utilities can be entry points for broader attacks. The process for exemptions should be transparent and clearly articulated.

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?

Cybersecurity incident reporting is already robust, with reporting requirements through NERC and Department of Energy ("DOE"), with the potential for new reporting expectations to be developed through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). The PUC should avoid adding to that burden by imposing separate reporting requirements and instead be open to receiving a copy of a standardized report form, such as the DOE Electric Emergency Incident and Disturbance Report (DOE-417) form. If information reported to another agency is not pertinent to the PUC, the utility should be permitted to redact sensitive information.

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?

Although CIRCIA and CISA's proposed rules do not require sharing cyber incident data with state commissions like the PUC, their implementation could still lead to regulatory overlap through parallel reporting obligations and differing definitions of reportable incidents, resulting in confusion, increased administrative burdens on utilities, and fragmented oversight. To avoid duplication and enhance coordination, the PUC should align its reporting requirements with federal standards and explore data-sharing agreements with CISA.

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?

To eliminate regulatory duplication, the Commission should clearly articulate the criteria for determining what assets are in-scope for new requirements. Any state requirements should clearly exclude assets already under FERC jurisdiction, per the NERC CIP Reliability Standards. Of those assets not covered by federal requirements, the PUC should create clear criteria to avoid applying unnecessary and excessive requirements to minimal risk assets. Specifically, the PUC should focus its requirements on electric distribution facilities and corporate systems with operational impact, related to sensitive information, or other high-risk factors. Reporting requirements should be limited to only those in-scope assets with material impacts on the electric distribution system.

As discussed in the response to earlier questions, the Commission should align its cybersecurity requirements with existing standards and reporting frameworks, such as the NIST framework, to ensure consistency and avoid redundant reporting. Finally, creating a unified compliance process and engaging stakeholders regularly will help streamline obligations and maintain regulatory clarity.

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.

Should the Commission move forward with the Staff Working Proposal to move cybersecurity protections to a separate chapter, the Company believes the remaining portions of Chapter 101 are sufficient to ensure protection of physical security,

emergency response, and business continuity. This response assumes that the newly created Chapters 103 and 104 sufficiently address cybersecurity risk.

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.

The Pennsylvania Regulatory Review Act requires that the Commission provide a cost estimate for "[T]he direct and indirect costs to the Commonwealth, to its political subdivisions and to the private sector." 71 P.S. §§ 745.5(a)(4). On the "benefits" side of the analysis, the Act requires the Commission to provide an evaluation of the benefits expected as a result of the regulation "when practicable." 71 P.S. §§ 745.5(a)(10). At this time, Duquesne Light does not offer any input on how the Commission should, and could, quantify the benefits of these proposed regulations. Regarding the costs, the Company emphasizes that an approach which relies on existing cybersecurity frameworks to the extent possible will provide the least cost implementation. To the extent the Commission attempts to quantify costs to the private sector resulting from the proposed Chapters 103 and 104, Duquesne Light recommends consulting with the Energy Association of Pennsylvania for implementation costs borne by its member utilities.

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.

Duquesne Light does not offer any additional considerations beyond those that have been raised through the previous questions.

IV. CONCLUSION

Duquesne Light appreciates the Commission's efforts to solicit and incorporate stakeholder feedback. Cybersecurity is one of the top risks to the utility sector. The Company complies with rigorous guidelines and expectations from NERC and the federal government, as well as industry best practice. It encourages the PUC to develop regulations that ensure utility compliance with these existing guidelines and regulations, rather than "recreating the wheel." Doing so ensures alignment with other agencies and states and represents an efficient use of resources by the Commission. The Company looks forward to continued collaboration on this critical issue.

Respectfully submitted,

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

July 16, 2025