341 White Pond Drive
Akron, OH 44320

Angelina Umstead, Esq.
(610) 921-6202
(330) 315-9263 (Fax)

July 16, 2025

VIA ELECTRONIC FILING

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

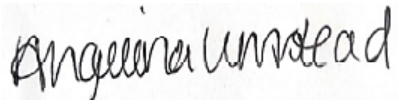
Re: Supplemental Advance Notice of Proposed Rulemaking Order to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting; Docket No. L-2022-3034353

Dear Secretary Homsher:

Pursuant to the Pennsylvania Public Utility Commission's Supplemental Advance Notice of Proposed Rulemaking Order entered on April 24, 2025, in the above-captioned proceeding, enclosed herewith for filing are the Comments of FirstEnergy Pennsylvania Electric Company.

Please contact me if you have any questions regarding this matter.

Very truly yours,



Angelina Umstead

AU/krak

Enclosures

c: Colin Scott, Law Bureau (Word version via email only)
Chris Van de Verg, Law Bureau (Word version via email only)
Daniel Searfoorce, Bureau of Technical Utility Services (Word version via email only)
Michael Holko, Office of Cybersecurity Compliance and Oversight (Word version via email only)
As Per Certificate of Service

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
FIRSTENERGY PENNSYLVANIA ELECTRIC COMPANY

I. INTRODUCTION

On April 24, 2025, the Pennsylvania Public Utility Commission ("Commission" or "PUC") entered the Supplemental Advance Notice of Proposed Rulemaking Order (the "Supplemental ANOPR") to review its current regulations relating to cybersecurity, which was subsequently published in the Pennsylvania Bulletin on May 17, 2025, under Docket No. L-2022-3034353. The PUC is seeking 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.

As directed by the Supplemental ANOPR, FirstEnergy Pennsylvania Electric Company ("FE PA" or "Company") respectfully submits the following response within 60 days of the Supplemental ANOPR's May 17, 2025 publication in the Pennsylvania Bulletin.

II. BACKGROUND

FE PA commends the Commission for recognizing the ever-evolving cybersecurity landscape and the importance of maintaining robust public utility cybersecurity fitness. Given the ever-shifting threat vectors, the Company fully supports the Commission's efforts to review

regulations relating to cyber-attack reporting and self-certification. Finding the correct approach is a difficult balancing act and is no easy task. Here again, the Company urges the Commission to consider a result-based approach rather than attempting to impose a one-size-fits-all approach to all uniquely situated Pennsylvania jurisdictional utilities.

III. COMMENTS

As requested by the Commission, the Company comments upon the questions in the Supplemental ANOPR Appendix A as follows.

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 80053, and/or NIST Special Publication 80082?

The Company supports the adoption of rules that require a cyber security program that is based on the National Institutes of Standards and Technologies ("NIST") Cyber Security Framework ("CSF") v2.0. The proposed rule in Chapter 103 contemplates, "[a]n annual cybersecurity evaluation which … uses … these assessments and standards … NIST CSF, NIST Special Publication 800-53, and NIST Special Publication 800-23 [ed]." While grounded in the framework's core principles, any adopted program should allow a company the flexibility to tailor its implementation to its specific circumstances. This approach ensures alignment with the NIST CSF's objectives while promoting practical and effective compliance.

It is also imperative to note that none of the above-referenced documents are prescriptive standards that are used "as is." For example, to effectively use NIST standards such as the NIST CSF or NIST 800-53, each company must interpret the standard's language such that it can be applied to their industry and situation. A company can then develop a cyber security program or map internal specification back into an existing cyber program. Ultimately, each company

maintains a unique cyber security program based on its unique interpretation of the relevant NIST standards.

Indeed, the NIST CSF is now broadly recognized as a complete framework for organizational cyber security risk management. Other states have adopted language where a program is based on the NIST CSF but does not mandate the NIST CSF in its exact form. This approach allows companies to interpret and implement the standard language in a way that aligns with their unique operations, risks, and industry context. By providing a flexible, principles-based foundation rather than a one-size-fits-all model, this approach allows companies to implement it in a way that is both relevant and practical to their specific needs.

Furthermore, while NIST Special Publication 800-53 and NIST Special Publication 800-82 provide useful guidance and examples of security policies, controls, and architectures, they do not rise to the level of a complete, assessable standard. Additionally, NIST SP800-82 Guide to Operational Technology is a generic document that contemplates a wide variety of implementation of "operational technology" devices. While this guidance can be useful to a jurisdictional utility, much of it is not necessarily directly applicable to a particular type of utility. For example, in the electric utility case, the use of "operational technology" has particular characteristics for timeliness and reliability that are special to the operation of electric power delivery.

Finally, and unique to the electric industry, the Commission should avoid overlap or interference with the North American Electric Reliability Corporation Critical Infrastructure Protection Standards ("NERC CIP"). Attestations that assets covered by NERC CIP should be permitted.

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?

The Company has no specific comment on Supplemental ANOPR Question 2.a.

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

Yes, the Commission should specify bright-line criteria for how waivers would be evaluated. The criteria should include how to handle overlapping federal regulations. This would allow utilities to understand the potential costs and regulatory requirements under the updated rules, if adopted.

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, the Commission should contemplate waivers for utility assets that are covered by other federal regulations. For example, assets that are covered by NERC CIP or the Transportation Security Administration's Pipeline Security Directives should be waived to the extent such regulations overlap with assets subject to Pennsylvania law. This approach avoids duplicative or conflicting requirements and allows utilities to focus resources on areas of higher risk. It also supports regulatory efficiency.

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?

The Company has no specific comment on Supplemental ANOPR Question 2.d.

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

Given that jurisdictional utilities have no ability to influence the evolution of the NIST CSF, the Commission should consider a company adopting the latest version of the NIST CSF as an expression of maturity as uncovered during the periodic PUC management audit rather than rulemaking proceeding that changes a required version number. Depending on the changes between versions of the NIST CSF, a non-trivial number of policies and procedures may need to be updated to use the correct terminology and concepts. For example, the process to adopt NIST CSF v2.0 from v1.0 by FirstEnergy Corp. took eighteen months of planning and execution to ensure that all updates were made consistently and fairly across a wide landscape of policies and controls. This also puts the urgency in a proper perspective. For instance, if a utility is already aligned with one version of the standard, it need not drop everything to comply with a future version. It allows for a risk-based and workload-sensitive approach to future adoption of standards. Similarly, the management audit is a safeguard to uncover utilities that are not keeping pace with the evolution of relevant standards over a reasonable period of time.

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

Any new self-certification process, similar to the one currently in place, should align directly with the needs and objectives of the Commission to protect the utility services and information of Commonwealth residents. The self-certification process allows the Commission to act in its regulatory oversight capacity by holding its jurisdictional utilities responsible for maintaining a proper cyber posture. It also provides a vehicle for addressing utility deficiencies in a reasonable and cost-effective manner without substantially increasing the regulatory burdens.

Additionally, the Commission's existing management audit process already serves as a sufficient mechanism for confirming compliance with cybersecurity requirements. Management

audits enable the Commission to gather relevant information regarding the Company's cybersecurity plans and programs. During these audits, the Company discusses its cyber programs extensively with staff. Through its comprehensive review of the Company's operations, including governance, risk management, and internal controls, the management audit provides the Commission with a robust framework to evaluate compliance.

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).

It is in everyone's best interest to keep the annual certifications confidential and treated as confidential security information ("CSI"), both in adherence to the required standards and non-adherers' certifications. For jurisdictional utilities that are attesting to compliance, there is minimal risk associated with the information in the filing. However, for jurisdictional utilities that are not compliant, this information would allow for target selection from motivated adversaries by enabling them to identify weaker potential targets. Cybercriminal groups increasingly conduct due diligence on organizations to help identify victims to target or support their ongoing tasks. While the attestations are not likely to contain significant tactical data within them, the strategic signals they send should be kept confidential.

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 Company suggests that the Commission accept reasonable forms of electronic filing, classified as CSI, for disclosure reasons. Assuming the annual certifications do not contain any amount of detail, stronger electronic protections are not needed.

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 Company finds that the Cybersecurity and Infrastructure Security Agency ("CISA") Notice of Proposed Rulemaking ("NOPR") to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022[1] ("CIRCIA"), has significant issues and supports the comments of the Edison Electric Institute ("EEI") filed on July 3, 2024.[2] The Commission should not seek to replicate or rely on CIRCIA for its regulatory oversight needs.

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)).

This task already is well-established by the commercial security industry at cost-effective pricing, through various sector-specific security organizations (*e.g.*, Electricity Information Sharing and Analysis Center ("E-ISAC"), Oil and Natural Energy Information Sharing and Analysis Center ("ONE-ISAC"), Water Information Sharing and Analysis Center ("WaterISAC"), etc.), and through the Department of Homeland Security CISA. The Commission establishing its own capability would be duplicative and not cost-effective for the Commonwealth.

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

See the Company's Response to Supplemental ANOPR Question 6.a.

[1] 6 U.S.C. § 681.
[2] https://www.regulations.gov/comment/CISA-2022-0010-0452.

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).

See the Company's Response to Supplemental ANOPR Question 6.a.

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).

See the Company's Response to Supplemental ANOPR Question 6.a.

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).

See the Company's Response to Supplemental ANOPR Question 6.a. Further, the Company would also oppose the use of "cyber incident data" in the furtherance of cybersecurity research. Such information is already widely available and at-scale such that the risk of accidental sharing of confidential information through a research program is much more of a concern than the availability of the data in general.

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?

This task already is well-established by the commercial security industry at cost-effective pricing, through various sector-specific security organizations (e.g., E-ISAC, ONE-ISAC, WaterISAC, etc.), and through industry partnerships (*e.g.*, EEI Cyber Mutual Assistance).

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

No, all public utilities should be required to report significant cyber security incidents to the Commission where the incident impacts delivery of utility services or requires notification to the Pennsylvania Attorney General under the state's breach notification law.

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?

To be effective, cyber information reporting must require the correct amount of specificity to avoid unrealistic and burdensome reporting requirements that will not ultimately provide regulators with the relevant information necessary to stay apprised of malicious breaches to the system. If the same documentation can be reused across regulatory jurisdictions, the Company recommends that the Commission accept reports in various formats. For example, should the Company need to file the Electric Emergency Incident and Disturbance Report (Form DOE-417) with the Department of Energy, it would be advantageous to the Company, to avoid duplication of effort, and the Commission, for rapidity of reporting, to reuse that format. To that end, it could be helpful and more efficient if the Commission permitted utilities to send a copy of cybersecurity incident reports submitted to other regulatory agencies to satisfy the reporting requirement.

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?

The Company finds the CISA NOPR to implement CIRCIA has significant issues and supports the comments of the EEI referenced above. In so far as duplication exists in form, the Company recommends that the Commission accept reports in various formats including any mandated by CIRCIA. As explained above in response to Question 8, it would be advantageous to

reuse that format. Otherwise, to be effective, such cyber reporting to the Commission must require the correct amount of specificity to avoid unrealistic and burdensome reporting requirements that will not ultimately provide regulators with the relevant information necessary to stay appraised of malicious breaches to the system.

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?

FirstEnergy Corp. and its subsidiaries are often active participants in cybersecurity proceedings in other states and thus have experience with other state utility commissions regarding public utility cybersecurity fitness and associated cost-benefit analysis undertaken in other jurisdictions. Consistent with its position in those proceedings, the Company advocates that state utility commissions hold jurisdictional utilities reasonably accountable for cybersecurity without creating undue burden.

For example, Maryland has promulgated the Code of Maryland Regulations Title 20, Subtitle 06 which requires adherence to the NIST Cyber Security Framework. Similarly, in New Jersey, the New Jersey Board of Public Utilities issued an Order wherein Jersey Central Power & Light Company, a FirstEnergy Corp. subsidiary, has a self-certification process for cybersecurity risks similar to considerations already in place in Pennsylvania and contemplated elsewhere in these comments.[3] Additionally, New Jersey Administrative Code, Title 14, Chapter 3 has enhanced requirements for transparent reporting of cyber security incidents to the state.

In sum, the Company advocates for rules that are risk-informed and tailored to reasonable compliance and uniform reporting requirements which are not duplicative of other jurisdictions.

[3] *I/M/O Utility Cyber Security Program Requirements*, BPU Docket No. A016030196, Order (March 18, 2016); https://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf.

The Company suggests that the Commission does not substantively deviate from other states or the guidance of the National Association of Regulatory Utility Commissions as doing so will translate to added costs for the purpose of completing and filling compliance paperwork. Aligning to the recommendations above should allow for a broad reuse of existing programs and practices.

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.

Beyond noting that cybersecurity is often synergistic with physical security and that cyber security issues may trigger emergency response and/or business continuity activities, the Company does not foresee any significant impact to physical security, emergency response and/or business continuity aspects in Chapter 101.

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 costs and benefits associated with the proposals will vary depending on the scope and prescriptiveness of final rules. For example, if the Commission adopts overly rigid requirements, the costs associated with compliance could be substantial. In contrast, a flexible risk-based framework that allows the utilities to tailor compliance to their specific systems and circumstances would result in lower compliance costs while still achieving meaningful cybersecurity benefits. This approach of evaluating the least burdensome alternative necessary to achieve the intended public policy objectives aligns with the Pennsylvania Regulatory Review Act.

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.

The Company's has a number of concerns and comments on the proposed language for Chapters 103 and 104 as set forth below.

IV. CHAPTER 103 COMMENTS

The Company offers the following comments relating to Chapter 103. Specifically, the Company believes that aligning certain definitions with other state and federal standards would promote consistency and avoid conflicting interpretations that create uncertainty.

The current definition of asset is overly broad and does not allow for a risk-based programmatic approach. The Company suggests replacing the definition of "Asset" with the following:

> *Asset* – Any combination of hardware, software, and related services, including industrial control systems ("ICS") that could affect a jurisdictional utility's consumer or system that stores information related to utility consumers and is protected pursuant to Pa. Cons. Statutes., Title. 73, Ch. 43 §§ 2301 – 2308.

Moreover, the Company suggests utilizing the term "asset" exclusively throughout Chapter 103. This would remove the following additional defined terms including, "information technology ('IT')", "operational technology ('OT')", and "supervisory control and data acquisition ('SCADA')."

Additionally, the Company suggests replacing the definition of "personal information" ("PI") with the statutory reference to personally identifiable information ("PII") used in the Pennsylvania Public Utility Code ("PA Code"). Replacing it with the definition used in the PA Code would promote clarity and consistency across the board. Further, using a uniform definition reduces the risk of conflicting interpretations and ensures utilities are operating under a common understanding of what constitutes protected information.

In addition to standardizing the definition section, the Company also believes that certain sections of Chapter 103 conflict with other chapters. To that end, the Company suggests removing language in Chapter 103 relating to "Continuity of Operations Plan ('COOP')" and "Disaster Recovery Plan ('DRP')" and add any strengthening the Commission feels is necessary to Chapter 101. A COOP or DRP is not simply a matter of cyber security. Indeed, there are many reasons a COOP or DRP may be required unrelated to cyber security. Additionally, the placement of this in Chapter 103 will be interpreted as a signal to jurisdictional utilities that COOP and DRP is a cybersecurity function when it is not and is potentially better handled by other parts of a utility. For example, at FirstEnergy, DRP is an IT function that is in response to any hazard. Similarly, a COOP, or "Business Continuity Plan" as referred to by FirstEnergy, is a holistic function of each business unit to remain in operation for key functions regardless of the reason of the interruption of the primary methods of executing that function.

Chapter 103 also presents some workability concerns. For example, the Company suggests that the Commission remove the language in Chapter 103 which mandates the use of the "Cybersecurity Evaluation Tool ('CSET')" and replace it with more generic language regarding the evaluation of coverage and maturity of a cybersecurity program. The CISA CSET is one possible tool in the toolbox for assessing cybersecurity. However, there are many other tools employed today that are just as effective. For example, the Company judges its cybersecurity through a combination of direct maturity assessment against the NIST CSF as well as use of a cyber risk quantification process. Neither are using the CSET, however, the Company believes its process is far more effective and comprehensive. Mandating the use of CSET by name is duplicative of existing, better processes and would create compliance paperwork of limited value.

Additionally, the definition of a "security management program" is too prescriptive. For example, mandates of "encryption at rest," enforcement of "application development best practices," and documentation of "all network traffic" is simplistic and does not lend itself to a risk-based approach leveraging defense-in-depth techniques. The definition should be broad and allow for a utility to demonstrate during an audit that its program is sufficient and workable leveraging the full scope of possible attributes. The following definition is suggested:

> *Cyber management program* – A documented plan by a utility that defines how a utility defends against and responds to cyber threats to Utility Computer Systems.

By utilizing this definition, the Commission can then judge effectiveness of a plan during the auditing process as a function of comprehensive coverage and maturity.

Moreover, consistent with the Company's comments above regarding the NIST CSF, the following replacement for 103.2(a) is offered:

(a) A Class 1 utility shall maintain and adhere to the following:

(i) A Cyber management program that is based on the NIST CSF that contains at least the following topics:

(A) A governance program.

(B) A security management program.

(C) A vulnerability management program.

(D) A risk management program.

(E) A threat management program.

(F) An incident response program.

(G) A recovery management program.

(ii) Assesses, itself or through a third-party, maturity and coverage of its Cyber management program.

The same definition can be used for Class 1, 2, 3, and 4 utilities simplifying the requirements. The Commission can then judge effectiveness of a plan during the auditing process as a function of comprehensive coverage and maturity.

Lastly with respect to Chapter 103, the Company urges the Commission to remove the language for 103.5 and treat adherence to revisions of the NIST CSF as an issue of maturity during audits. Please see the Company's comprehensive comment in Question 2(c) above for a fulsome explanation of why this section is unworkable.

V. CHAPTER 104 COMMENTS

Similar to the Company's comments relating to Chapter 103, the Company recommends that the definitions in Chapter 104 align with other state and federal standards. For example, the proposed definition of "cyber incident" is overly broad and will result in substantial amounts of unnecessary reporting to the Commission and the Pennsylvania Criminal Intelligence Center. For this reason, the Company suggests replacing the definition of "cyber incident" with the following:

> *Cyber Incident* – A successful, intentional, malicious bypass, or compromise of one or more security controls of a Utility Computer System resulting in:
>
> (1) A breach or degradation of the confidentiality, integrity, or availability of an Asset;
> (2) An otherwise-authorized user exceeding authorized levels of access; or
> (3) Malicious exposure of data protected specified in Pa. Cons. Statutes., Title. 73, Ch. 43 §§ 2301 2308.

Additionally, and consistent with the comments above relating to Chapter 103, the Company suggests replacing the definition of "asset" with the recommended definition set forth above. The Company also proposes replacing the definition of PI with the statutory reference to PII used in the PA Code as previously explained above.

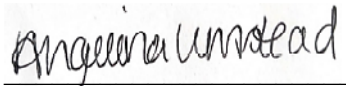
Lastly with respect to Chapter 104, the Company encourages the Commission to remove language in Chapter 104.2(a)(iv) regarding "potential compromise." A jurisdictional utility is not in a position to determine if its risk or incident is a risk to any other entity. Such assessments require access to information and visibility beyond a utility's control. Such assessments are more appropriately conducted by federal or state agencies with greater authority and visibility.

VI. CONCLUSION

FirstEnergy Pennsylvania Electric Company appreciates the opportunity to provide comments to the Commission in response to the Supplemental ANOPR, and the advancement of this proceeding. The Company looks forward to further collaboration and discussion with the Commission and interested stakeholders on this important topic.

Respectfully submitted,

Dated: July 16, 2025



Angelina Umstead
Attorney No. 309615
FirstEnergy Service Company
341 White Pond Drive
Akron, OH 44320
(610) 921-6202
aumstead@firstenergycorp.com

Counsel for FirstEnergy Pennsylvania Electric Company

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**

CERTIFICATE OF SERVICE

I hereby certify that I have this day served a true and correct copy of the foregoing document upon the individuals listed below, in accordance with the requirements of 52 Pa. Code § 1.54 (relating to service by a participant).

Service by electronic mail only as follows:

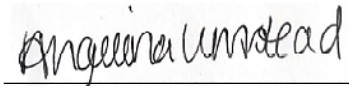
NazAarah Sabree
Office of Small Business Advocate
555 Walnut Street
Forum Place, 1st Floor
Harrisburg, PA 17101
ra-sba@pa.gov
tereswagne@pa.gov

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

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

Patti Kay Wisniewski Regulatory Agent
1600 JFK Boulevard
4 Penn Center
Philadelphia, PA 19103
Wisniewski.patti-kay@epa.gov

Dated: July 16, 2025



Angelina Umstead
FirstEnergy Service Company
341 White Pond Drive
Akron, OH 44320
(610) 921-6202
aumstead@firstenergycorp.com

Counsel for FirstEnergy Pennsylvania Electric Company