AN EXELON COMPANY

Jack R. Garfinkle
Associate General Counsel
2301 Market Street / S23-1
Philadelphia, PA 19103

Direct Dial: 267-533-1999
Email: Jack.Garfinkle@exeloncorp.com

July 16, 2025

VIA ELECTRONIC FILING

Matthew L. Homsher, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street
Harrisburg, PA 17120

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

Dear Secretary Homsher:

Enclosed please find the **Comments of PECO Energy Company ("Comments")** for filing in the above-referenced docket.

Copies of these Comments have been served on the parties as indicated on the enclosed Certificate of Service.

If you have any questions regarding this filing, please do not hesitate to contact me at 267-533-1999.

Very truly yours,

Jack R. Garfinkle

Enclosures

Cc: Colin Scott, Assistant Counsel, Law Bureau colinscott@pa.gov
Chris Van de Verg, Deputy Chief Counsel, Law Bureau cvandeverg@pa.gov
Daniel Searfoorce, Manager (BTUS) dsearfoorc@pa.gov
Michael Holko, Director, 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**

CERTIFICATE OF SERVICE

I hereby certify that on this date, a true and correct copy of the foregoing Comments 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 E-MAIL ONLY

Allison Kaster, Chief Prosecutor
Bureau of Investigation and Enforcement
Commonwealth Keystone Building
400 North Street, 2nd Floor West
PO Box 3265
Harrisburg, PA 17105-3265
akaster@pa.gov

Candis A. Tunilo, Sr. Counsel
NiSource Corporate Services Company
800 N. Third Street,
Suite 204
Harrisburg, PA 17102
ctunilo@nisource.com

NazAarah Sabree,
Small Business Advocate
Office of Small Business Advocate
555 Walnut Street 1st Floor, Forum Place
Harrisburg, PA 17101-1923
nsabree@pa.gov
ra-sba@pa.gov

Donna M.J. Clark, V.P. & General Counsel
Nicole W. Luciano, CAE, IOM Director of Policy
Energy Association of PA
800 N. Third Street, Suite 205
Harrisburg, PA 17102-2025
dclark@energypa.org
nluciano@energypa.org

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

Darsh Singh, Esq.
First Energy / Met-Ed
2800 Pottsville Pike
P.O. Box 16001
Reading, PA 19612
singhd@firstenergycorp.com

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

Pamela C. Polacek, Chief Legal & Regulatory Officer
CT Enterprises, Inc.
1775 Industrial Blvd.
Lewisburg, PA 17837
ppolacek@ctenterprises.org

Kimberly A. Klock, Assistant General Counsel
PPL
Two North Ninth Street
Allentown, PA 18101-1179
kklock@pplweb.com

Kevin Sunday, Director Government Affairs
PA Chamber of Business and Industry
417 Walnut Street
Harrisburg, PA 17101
ksunday@pachamber.org

Lindsay A. Baxter, Sr. Manger Policy & Public Affairs
Duquesne Light Company
411 Seventh Avenue, MailDrop 15-7
Pittsburgh, PA 15219
lbaxter@duquesnelight.com

Meagan B. Moore, Esq.
PNG Companies LLC
375 North Shore Drive
Pittsburgh, PA 15212
Meagan.moore@peoples-gas.com

Dated: July 16, 2025

Jack R. Garfinkle, Esq. (Pa Attorney No. 81892)
Counsel for PECO Energy Company
2301 Market Street, 23rd Floor
Philadelphia, PA 19103
(267)-533-1999
jack.garfinkle@exeloncorp.com

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

RULEMAKING TO REVIEW CYBER SECURITY SELF- CERTIFICATION REQUIREMENTS AND THE CRITERIA FOR CYBER ATTACK REPORTING

L-2022-3034353

COMMENTS OF PECO ENERGY COMPANY

On April 24, 2025, the Pennsylvania Public Utility Commission (the "Commission" or the "PUC") entered a Supplemental Advance Notice of Proposed Rulemaking Order ("ANOPR") in the above-captioned docket to further review its current regulations relating to cybersecurity. This follows the Nov. 10, 2022, adoption of an Advance Notice of Proposed Rulemaking in Docket L-2022-3034353, *Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting* ("2022 ANOPR"). PECO Energy Company ("PECO") submitted comments in accordance with the 2022 ANOPR on February 8, 2023, and submits these comments in accordance with the ANOPR.[1]

PECO is a combined electric and gas distribution utility company committed to delivering energy safely, reliably, and affordably to the communities it serves. PECO and its parent company, Exelon Corporation ("Exelon"), recognize the importance of implementing cybersecurity controls consistent with established and evolving security standards to protect critical infrastructure and maintain safe, reliable, and affordable energy delivery. The rapidly evolving nature of cybersecurity threats poses unique challenges for the critical infrastructure community, including utilities, and warrants careful consideration.

PECO appreciates the efforts of the Commission to evaluate opportunities to improve its cybersecurity program framework. In these supplemental comments, PECO provides responses to

[1] PECO Energy Co., Comment Letter on Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Docket No. L-2022-3034353 (Feb. 8, 2023).

the Commission's questions presented in the ANOPR regarding proposed changes to the Commission's cybersecurity regulations, including self-certification requirements and the criteria for cyber incident reporting, while referring to the Staff Working Proposals provided in Appendix B of the ANOPR.

PECO recommends that the Commission focus on two foundational points as it reviews comments submitted in response to the Supplemental ANOPR, which are highlighted in the Executive Summary below—first, that the Commission's cybersecurity fitness standards should align to the NIST Cybersecurity Framework, and secondly, that the Commission should adopt incident reporting requirements only when there is impact to actual operations or customer information. In the remainder of these comments, PECO provides detailed responses to the questions presented in the ANOPR. PECO looks forward to working with the Commission and all stakeholders to continue protecting the Commonwealth's critical infrastructure and ensuring safe, continuous, and reliable utility service.

I. EXECUTIVE SUMMARY

A. The Commission's Cybersecurity Fitness Standards Should Align to The NIST Cybersecurity Framework

PECO strongly supports the Commission's adoption of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("NIST CSF") as the foundational framework for the Commission's oversight of utilities' cybersecurity fitness. NIST CSF offers a flexible, risk-based model that empowers utilities of all sizes to tailor protections to their unique operational situations, rather than prescribe specific technical procedures that may be duplicative of existing federal requirements or ill-suited to the cyber risks to particular infrastructure. PECO believes that the Commission, public utilities, and customers will be best served if the Commission allows utilities to align their cybersecurity programs to NIST CSF.

In a similar vein, rather than imposing separate top-down requirements where appropriate cyber controls already exist for particular assets, and where applicable the Commission should accept compliance with federal regulations for utility assets under the jurisdiction of federal agencies to decrease administrative burdens and avoid duplication. For example, assets subject to mandatory critical infrastructure protection reliability standards developed by the North American Electric Reliability Corporation ("NERC") should not be subject to overlapping, separately Commission requirements. When there are NERC mandates in place, separate Commission requirements would significantly complicate compliance implementation and documentation without materially contributing to the cybersecurity of those assets. If a public utility is following existing mandated controls, such as controls for the authentication of remote access to cyber assets, additional remote access control requirements are unnecessary.

Adopting the NIST CSF would allow public utilities to rely on those existing federal regulations to provide the necessary identifying, protecting, detecting, responding, and recovering controls where the existing regulations apply, while empowering public utilities to implement NIST CSF controls for assets not subject to existing regulatory requirements.

B. The Commission Should Adopt Incident Reporting Requirements Only When There is Impact to Actual Operations or Customer Information

Given the numerous legal and regulatory requirements applicable to cybersecurity, especially in incident response and reporting, there is significant potential for conflict, overlap, or duplication of terms and concepts. Accordingly, PECO urges the Commission to refine the definition of *Cyber Incident* and the *Reporting Requirements* in the Staff Working Proposal so they match the scope of its statutory role by requiring the reporting only of cyber incidents that actually compromise operations or expose customer PI. For efficiency, the Commission should also allow

utilities to leverage reports used to comply with existing federal cyber incident reporting requirements.

When an incident occurs, public utilities already have a very short window of time to verify information about the incident and report it to various regulators, and in some cases law enforcement and intelligence agencies. As a result, complex and detailed procedures are in place to prepare to handle incident investigation and reporting on a very short timeframe. Because those reports differ in their substance, reporting is already legally complex as utilities must make sure each report contains the exact data required for that particular report. Rather than adding slightly different reporting requirements, the Commission can achieve its regulatory objective on transparency regarding these incidents without adding to the reporting complexity and burden by allowing public utilities to use their existing federal cyber incident reports when reporting incidents to the Commission.

II. RESPONSE TO THE QUESTIONS PRESENTED IN THE SUPPLEMENTAL ANOPR

Question No. 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?

PECO recommends that the Commission require jurisdictional utilities to "align" their cybersecurity programs and plans specifically with the NIST Cybersecurity Framework ("NIST CSF") for assets used to provide public utility service in Pennsylvania that are not already regulated by federal entities and accept compliance with federal regulations for those that are so regulated.[2] This approach is appropriate because it allows utilities to leverage the strengths of their

[2] PECO distinguishes the term "align" here from "conform" as used in Question #1, which PECO interprets to imply compliance. Industry standards, such as NIST CSF, are voluntary frameworks from which entities can select and tailor appropriate features to configure their own cybersecurity programs in a manner specific to the unique nature

existing regulated programs, which are rigorously audited and based on mature federal models, while avoiding potentially duplicative or conflicting controls. An example of the application of this approach is PECO which, like other Pennsylvania utilities, is already subject to comprehensive cybersecurity requirements promulgated by NERC and the Transportation Security Administration ("TSA") for their most critical IT and OT systems. Along with other Exelon utilities, PECO utilizes a NIST CSF-based cybersecurity program that both supports compliance with these federal requirements and effectively secures all remaining Information Technology ("IT") and Operational Technology ("OT") systems. This approach also provides utilities with flexibility to manage cybersecurity risks for the balance of assets that are not currently subject to federal regulation. The NIST CSF is particularly well suited in this regard because, in addition to being a flexible, risk-based framework, the NIST CSF is industry agnostic and was developed to help a wide variety of organizations manage and reduce cybersecurity risks. As such, it will be adaptable to jurisdictional utilities of all types and sizes, regardless of sector or cyber maturity level.

Another reason the NIST CSF is well suited for this task is because it is already well established and recognized as the industry standard for cybersecurity. For instance, the National Association of Regulatory Utility Commissioners' ("NARUC") *Cybersecurity Baselines for Electric Distribution Systems and DER* ("Cybersecurity Baselines") are structured to offer guidance to critical infrastructure owner and operators in best practices for the distribution system and the distributed energy resources ("DERs") that connect to them.[3] NARUC's Cybersecurity Baselines are based on the five core functions of the NIST CSF (v1.1). Rather than mandating

---

and risks of their operations. As such, an entity would not comply (or conform) with a standard, but instead would align their program configuration to it. In addition, the language in such standards is replete with discretionary conditions and ambiguous language that is generally incompatible with audits.

[3] National Ass'n of Regulatory Utility Comm'rs, "Cybersecurity Baselines for Electric Distribution Systems and DER," NARUC (last visited July 2, 2025), https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/.

specific technologies or controls, NARUC's baselines encourage risk-based decision making and performance-based metrics that focus on security outcomes. PECO notes that NARUC rejected a more prescriptive approach when developing the Cybersecurity Baselines due to the impossibility of creating a "one-size-fits-all" approach to cybersecurity fitness. The purpose of NARUC's Cybersecurity Baselines is to assist entities wishing to adopt foundational requirements of a cybersecurity risk management program. These entities include state public utility commissions and other oversight bodies like state energy offices and state legislators. The Cybersecurity Baselines encourage alignment with other federal standards and risk-based approaches to cybersecurity based on a company's unique set of assets and circumstances. And so, the Commission's initiative to align with NIST CSF is consistent with NARUC's approach.

While NIST Special Publications, such as SP 800-53 and SP 800-52, also offer the benefit of standardization, PECO recommends against the Commission's adoption of these and other similar publications. The NIST Special Publications include specific technical controls that were designed to satisfy minimum requirements for federal information systems (e.g., Federal Information Processing Standards, Federal Information Security Modernization Act requirements) that in most cases will not be directly applicable to Commission-jurisdictional utilities. In addition, the implementation of these controls may not be necessary or feasible for Commission-regulated utilities. While the NIST Special Publications may serve as valuable resources to support NIST CSF-based programs, PECO submits that the Special Publications should not be adopted in this proceeding or otherwise required by the Commission to be implemented as a baseline set of standards.[4]

[4] See, e.g., *Nat'l Inst. of Standards & Tech.,* "Informative References: What Are They, and How Are They Used?," *Cybersecurity Framework Resource Center (July 2, 2017),* https://www.nist.gov/cyberframework/online-learning/informative-references?utm_source=chatgpt.com.

Allowing utilities to demonstrate compliance with federal regulations where they apply, then allow alignment with NIST CSF to demonstrate cybersecurity fitness for their remaining assets that are used to provide public utility service in Pennsylvania, will close the security gap identified by the Commission in the ANOPR, support self-certification, decrease administrative burden for both the Commission and utilities, and avoid duplicative compliance burdens with federal requirements.[5] Other jurisdictions, like Maryland, have successfully employed this approach (*see* PECO's response to Question #2a).[6]

As previously stated in its 2022 ANOPR comments, PECO respectfully submits that the Commission should avoid imposing requirements that force utilities to duplicate the controls that they are already implementing in other regulatory efforts and programs.[7] Instead, allowing jurisdictional utilities certify compliance with federal cybersecurity requirements and align their cybersecurity programs with NIST CSF for their remaining systems would serve this purpose while providing efficient and effective cybersecurity for all systems.

> *Question No. 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?*

[5] *See* Pa. Pub. Util. Comm'n, Supplemental Advance Notice of Proposed Rulemaking Order, Docket No. M-2025-302425, at 13 (Apr. 24, 2025) (identifying gaps in the cybersecurity standards regimes maintained by federal sector specific agencies).

[6] *See* Md. Code Regs. tit. 20, subtit. 06 (describing MD PUC approach of allowing alignment with frameworks like NIST CSF, allowing self-certifications, accepting federal regulatory audits for assets covered by them, allowing onsite document retention for review, and requiring periodic assessments and reporting).

[7] PECO Energy Co., Comment Letter on Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Docket No. L-2022-3034353, at 8 (Feb. 8, 2023).

If the Commission were to adopt the aforementioned approach and allow jurisdictional utilities to align the aspects of their cybersecurity programs that are not currently federally regulated with NIST CSF, PECO does not believe the Commission would need to classify individual utilities by size or capability. As previously discussed in Question #1, NIST CSF offers a flexible, risk-based model that can be tailored to the entity's unique operational requirements, including those driven by size, capability, and cyber risk. By adopting an outcome-based approach that leverages NIST CSF, there should be no need to classify utilities by size or function, which would simplify both the text and implementation of the new rule while ensuring that the controls are suited to the risk faced by a public utility along a spectrum, rather in predefined tranches that may or may not adequately match the public utility's actual risk.

The relative simplicity of this approach is demonstrated by the State of Maryland, Public Service Commission in its cybersecurity regulations.[8] Maryland's rule, which was updated in 2025 after a comprehensive, multi-year, collaborative rulemaking process, requires jurisdictional utilities to "align their cybersecurity practices" to a standard that can be based on NIST CSF, resulting in a relatively straightforward regulation for governing cybersecurity programs that does not need to classify utilities by any metric:

> **Md. Code Regs. 20.06.01.03 - Good Cybersecurity Practice**
>
> A. All public service companies shall follow good cybersecurity practice.
>
> B. At a minimum, public service company cybersecurity plans shall address cybersecurity-related governance, risk management, procurement practices, personnel hiring, training policies, situational awareness, response, recovery, zero trust implementation, and transparent reporting of cybersecurity incidents to State and federal entities.

[8] *See* Md. Code Regs. tit. 20, subtit. 06 (2025).

> C. At a minimum, all public service companies shall comply with all cybersecurity standards applicable to their cybersecurity devices **and align their cybersecurity practices with** Cybersecurity and Infrastructure Security Agency's Cross-Sector Cybersecurity Performance Goals (CPG) or **a more stringent standard that is based on the National Institute of Standards and Technology (NIST) security frameworks.**[9]

This approach likewise simplifies the subsequent section of Maryland's rule regarding periodic assessments and reporting, avoiding the need for classifications in these contexts as well.[10] By contrast, the Staff Working Proposals in this current ANOPR require the utilities and the Commission to deal with at least five different utility classes in the contexts of definitions, evaluations, programs, and certifications, a much more complex and burdensome construction.[11]

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

As a general matter, PECO believes it would be beneficial for the Commission to clarify the criteria it may consider when reviewing a waiver petition.

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?

Waivers should not be necessary if a utility uses equal or stricter standards than NIST CSF. Maryland included that option by rule (*see* Question #2a).

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?

As previously discussed, NIST CSF allows the tailoring of cybersecurity programs for entities of all sizes, based upon operational needs, maturity, and risk, and so size-based waivers should not be unnecessary.

---

[9] *See* Md. Code Regs. 20.06.01.03 (2025); *id* (*emphasis added*).
[10] *See* Md. Code Regs. 20.06.01.07 (2025).
[11] *See* Pa. Pub. Util. Comm'n, Supplemental Advance Notice of Proposed Rulemaking Order, Docket No. M-2025-302425, at Appendix B (Apr. 24, 2025).

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

PECO recommends that the Commission account for changes and updates by monitoring utility compliance through the self-certification process. Doing so will ensure jurisdictional utilities have considered the most current NIST CSF version as part of their cybersecurity plans and programs.

The Commission should also take steps to assist utilities stay informed of developments in the framework and in soliciting feedback on proposed changes and guidance. Given the speed at which technology and cyber risk evolves and the increasing digitization of the utility industry, any standards and frameworks must evolve as well. Ongoing, close communication between the Commission and its regulated community will help ensure the standards and frameworks reflect the use of technology and appropriate cyber controls to protect that technology. PECO anticipates that any standards and frameworks in this area will need to be iterative. Coordination between the Commission and utilities will provide the Commission with insight for revising those requirements when and as appropriate and will better assist utilities in understanding and implementing the Commission's requirements.

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

PECO recommends that the Commission continue its current self-certification approach to confirm compliance with Commonwealth cybersecurity requirements. Specifically, the new rule should require jurisdictional utilities to self-certify compliance with federal cybersecurity regulations where applicable, and to alignment with NIST CSF for their remaining assets that are used to provide public utility service in Pennsylvania.

Allowing utilities to self-certify compliance with the Commission's security objectives through implementation of other appropriate federal or industry standards would continue to preserve the Commission's longstanding objectives to avoid replicating regulations that were already in place and required by the federal government or other agencies. Additionally, this approach would allow the Commission to ensure adherence to good cybersecurity fitness for utility assets, while permitting the utilities to tailor their cybersecurity programs according to their size, sector, and maturity level, and with the added benefit of preserving administrative resources for both the Commission and utilities.

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

PECO recommends that the Commission adopt an enforcement framework that prioritizes remediation of identified vulnerabilities over compliance administration and civil penalties, particularly for violations that do not pose a serious or significant risk to utility operations. PECO believes that resolving instances of potential noncompliance in this manner ensures that utilities continually evaluate their compliance with the Commission's requirements while focusing their resources on maintaining a strong cybersecurity posture.

These remediation-centered frameworks have worked well in other regulated programs. For example, TSA employs a progressive approach to compliance enforcement and utilizes its Action Plan program, which is a collaborative alternative to civil penalties, and which has worked successfully, both for TSA's established regulatory programs, and its newly established cybersecurity security directives.[12]

---

[12] See U.S. DEP'T OF HOMELAND SEC., TRANSP. SEC. ADMIN., *TSA Action Plan Program* (technical change issued Dec. 12, 2022) (describing TSA's voluntary Action Plan Program as part of a progressive civil enforcement policy), https://www.tsa.gov/sites/default/files/action_plan_program.pdf; *see* U.S. GOV'T ACCOUNTABILITY OFFICE, *Surface Transportation: TSA Is Taking Steps to Enhance Cybersecurity, but Additional Actions Are Needed* 5-6 tbl. 1, GAO-25-107947 (Apr. 30, 2025) (demonstrating the various transportation modes added to TSA's cybersecurity regulatory program, which includes the Action Plan Program, https://www.gao.gov/assets/880/873943.pdf.

TSA's Action Plan Program is part of TSA's progressive civil enforcement framework.

> TSA's Action Plan Program provides an opportunity for eligible parties and TSA to discuss and reach an agreement on corrective actions to address the root cause of any [qualifying] security vulnerability or noncompliance with TSA's security requirements…and resolve that vulnerability or noncompliance with administrative action instead of a civil enforcement action.[13]

This program incentivizes eligible parties to identify security vulnerabilities, correct their own instances of regulatory noncompliance, invest resources and effort to improve security, and increases partnerships between TSA and industry stakeholders.[14] The program does exclude certain vulnerabilities or instances of noncompliance, including those that are egregious, intentional, or involve criminal activity or fraud.[15]

Another example of this approach is NERC Reliability Standards in which violations that are not pursued through an enforcement action are recorded by regulated utilities as "Compliance Exceptions." This NERC program allows regional regulatory bodies to exercise their enforcement discretion over instances of noncompliance that pose a minimal risk to reliability and therefore do not warrant financial penalties. Compliance Exception treatment is particularly appropriate if the utility adequately identifies its noncompliance, assesses the risk properly as minimal risk, and mitigates the violation in a timely and appropriate manner.[16] Additionally, NERC's self-logging program allows utilities to self-monitor and mitigate instances of noncompliance to log minimal risk violations that would otherwise be individually self-reported.[17] These programs allows utilities to self-correct violations and develop robust internal compliance program and management

[13] *Id*, at 1.
[14] *See id*. at 1.
[15] *See id*. at 5.
[16] *See* NERC, Rules of Procedure, App. 4C, Section 4A.0.
[17] *See* NERC, Rules of Procedure, App. 4C, Section 4.5.

practices that are informed by prior violations, while fostering efficiency for both the regulated entity and the regulator through the reduction of formal enforcement processes.

PECO recommends that the Commission consider a similar approach for enforcement of its cybersecurity requirements that prioritizes remediation, long-term improvements to cybersecurity posture, and administrative efficiency.

> *Question No. 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- 214.6 (CSI Act).*

PECO requests that annual certifications submitted by Pennsylvania public utilities, whether redacted or not, be considered confidential security information ("CSI"), be handled as such, and not be disclosed to the public. In Pennsylvania, CSI is defined as

> Information contained within a record maintained by an agency in any form, the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, public property or public utility facilities...[18]

On this point, PECO respectfully requests that the Commission carefully consider the deliberations of FERC and NERC on a substantially similar issue in a NERC administrative docket.[19] In this docket, FERC and NERC staff determined that publishing redacted cybersecurity violation and penalty information poses a tangible risk to the electric grid and that considering the growing threat environment such information should be kept confidential.[20]

---

[18] 52 Pa. Code § 102.2 (2025) (defining "confidential security information").
[19] *See* FERC Docket No. AD19-18-000 (*Second Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards*) (Sept. 23, 2020) https://www.ferc.gov/media/second-joint-staff-white-paper-notices-penalty-pertaining-violations-critical-infrastructure.
[20] *See id.*

Likewise, the public release or unsecure transmission of even redacted certifications by Pennsylvania public utilities that indicate alignment/non-alignment with NIST CSF (or other standards), or compliance/non-compliance with federal regulatory requirements would pose a tangible cybersecurity risk to their facilities in the form of their IT and OT systems. Thus, the Commission should consider annual certifications submitted by public utilities as CSI and protect them as required by Pennsylvania law, even if redacted.[21]

> *Question No. 4: If an annual certification should be considered CSI, what procedures should the Commission follow to security accept electronic filing of certifications consistent with the CSI Act*[22]*?*

Pennsylvania law does not currently allow the electronic submission of records containing CSI by jurisdictional utilities, but the Commission could revise 52 Pa. Code to allow electronic submission of annual cybersecurity certifications and then establish a secure portal to accept the submissions.[23] Alternatively, PECO proposes that it may be more efficient for the Commission to allow utilities to electronically file non-CSI certifications that their required compliance documentation is present onsite and up-to-date, pursuant to Pennsylvania law.[24]

Pursuant to 52 Pa. Code §102.3(g) – *Electronic submissions*, "The Commission does not authorize the use of e-mail or any other electronic mail system to transmit records containing confidential security information."[25] Therefore, under current Pennsylvania law, utilities may not submit CSI annual cybersecurity certifications electronically. To allow electronic filing, the Commission could revise 52 Pa. Code §102.3, as part of the current rulemaking, to allow the

---

[21] This is a revised position regarding the sensitivity of cybersecurity certifications from that expressed in comments PECO filed in response to the Commission's initial 2022 ANOPR, and reflects consideration of the FERC administrative docket; *see id.; see* PECO Energy Co., Comment Letter on Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Docket No. L-2022-3034353, at 13 (Feb. 8, 2023).

[22] 2006 Act 156 - The Official Website of the Pennsylvania General Assembly

[23] *See* 52 Pa. Code §102.3(g).

[24] *See* 52 Pa. Code §102.3(a).

[25] 52 Pa. Code §102.3(g).

electronic transmission of CSI information and then designate a secure transmission method, ideally a secure portal.

Alternatively, PECO proposes that a more efficient approach would be for the Commission to accept non-CSI certifications from utilities stating that their annual cybersecurity certifications, as well as other required compliance documents, are onsite and up to date. 52 Pa. Code §102.3 states that, unless directed otherwise by the Commission, utilities may maintain records containing CSI onsite and "[c]ertify that the record is present and up-to-date," pending review by the Commission.[26] There are no noted restrictions on the electronic transmission of those types of non-CSI certifications, so they could ideally be emailed to the Commission.

This approach would be consistent with PECO's stated preference that the Commission conduct onsite reviews of compliance records, rather than requiring their submission, to avoid the security risks inherent in aggregating substantial amounts of CSI, from multiple utilities, in a single location.[27]

> *Question No. 5: Are the purposes and design for cyber incident report collection stated by CISA, NOPR at Section III. C. ("Purpose of Regulation")[28], substantially the same as the Commission's statutory role in ensuring the jurisdictional utilities provide reasonably adequate, reliable, continuous, and safe service to the public?*

PECO asserts that the statutory role of the Commission, in the context of cyber incident reporting, is narrower than that of CISA, and thus the Commission's cyber incident reporting framework should be tailored more narrowly than currently in the Staff Working Proposals, such

[26] *See* 52 Pa. Code §102.3(a)(1)-(3)
[27] PECO Energy Co., Comment Letter on Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Docket No. L-2022-3034353, at 10 (Feb. 8, 2023).
[28] Federal Register :: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

that only actual incidents that cause actual effects and serve the Commission's statutory role are reported.[29]

CISA's stated purpose for its cyber incident report collection is to collect a large volume of incident reports "to support reliable trend analysis, vulnerability identification, provision of early warnings, and other key purposes … as indicated by CIRCIA." [30] To this purpose, CISA designed its cyber incident report collection to include this proposed this definition:

> *Cyber incident* means an occurrence that **actually** jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or **actually** jeopardizes, without lawful authority, an information system."[31]

By contrast, the purpose of the Commission's incident reporting regulations is "limited to keeping the Commission abreast of service affecting impacts for continuity of operations and continuity of government (COOP/COG) purposes, and ensuring continuous public utility service to Pennsylvania residents and businesses."[32] Yet, the Staff Working Proposal definition of Cyber Incident is similar to CISA's, and in fact more expansive:

> *Cyber incident*—An occurrence that **actually or imminently** compromises or jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or **actually or imminently** compromises or jeopardizes, without lawful authority, proper attribution or operation of, or control over, operational technology. This term includes any instance of ransomware.[33]

---

[29] *See* Pa. Pub. Util. Comm'n, Supplemental Advance Notice of Proposed Rulemaking Order, Docket No. M-2025-302425, at 16-17, Appendix B (Apr. 24, 2025).
[30] *See* Pa. Pub. Util. Comm'n, Supplemental Advance Notice of Proposed Rulemaking Order, Docket No. M-2025-302425, at 16-17 (Apr. 24, 2025).
[31] DHS CISA, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Federal Register Vol. 89, No. 66 at 23766 (Apr. 4, 2024).
[32] *See* Pa. Pub. Util. Comm'n, Supplemental Advance Notice of Proposed Rulemaking Order, Docket No. M-2025-302425, at 17 (Apr. 24, 2025) (citing Joint Statement of Chairperson Robert F. Powelson and Vice Chairperson John F. Coleman, Pa. PUC Docket No. L20092104274, Utilities' Service Outage Response and Restoration Practices, Pa.B. Vol. 42, Number 1, at 9, 20 (Jan. 7, 2012)).
[33] Pa. Pub. Util. Comm'n, Supplemental Advance Notice of Proposed Rulemaking Order, Docket No. M-2025-302425, at Appendix B (Apr. 24, 2025).

Specifically, the inclusion of the word "imminent," as opposed to only "actual," in the cyber incident definition expands the scope of reportable cyber incidents beyond those required by CISA.

In addition, unlike CISA, which requires at least one of four actual deleterious effects to occur to make a cyber incident reportable, the Staff Working Proposal requires reporting for any "**risk for potential compromise** of IT or OT owned, controlled or managed by, or serving, entities other than the reporting public utility, including customers, **third parties**, the Commission or other public utilities."[34] PECO believes that "risk for potential compromise" makes this criterion nebulous and overbroad and will lead to overreporting and arbitrary enforcement, as will the inclusion of unnamed "third parties."

Furthermore, the use of "imminent" or "risk of" in reference to compromise or jeopardy of information systems or operational technology will also require utilities to make judgment calls about whether a particular incident is "imminent" and therefore is likely to lead to conservative over-reporting. This will maximize the quantity but reduce the overall usefulness of the incident reports received by the Commission. Incident reporting triggered by actual impacts is much more quantitative and will provide the Commission with relevant and useful information.

PECO recommends that the Commission more narrowly tailor its cyber incident reporting framework to its statutory role of ensuring the adequate, reliable, continuous, and safe utility service to the public by requiring reporting of only those events that cause actual effects that negatively impact the "continuous public utility service to Pennsylvania residents and businesses."

Question No. 6: Identify any role you believe the Commission has to play in each of the following areas:

34

The Commission plays an important role in the oversight of public utilities in the Commonwealth and should remain informed on the threats facing utilities. PECO stands ready to collaborate with the Commission to support cybersecurity and resiliency in the Commonwealth, but respectfully submits that it is not necessary for the Commission to engage in several of the activities described below. As discussed below, these activities, such as trending and tracking threat analysis, reflect functions already performed internally by utilities and through partnerships with federal government associations and the commercial security industry. However, given the ongoing realignment and restructuring of federal agencies, the Commission may have future roles to play in these areas.[35]

a. *Trend and track 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 *TTOs).*

This is provided by CISA, and through Information Sharing and Analysis Centers such as the Electricity (E-ISAC) and the Distributed Natural Gas (DNG-ISAC). The Mitre Corporation (commonly known as "MITRE") is another source that provides a matrix and log of historical 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)*

CISA provides publicly available Known Exploited Vulnerabilities (KEV) which provides information on security flaws and software weaknesses that are known to have been exposed and leveraged by attackers. These are known because they have been involved in incident response cases conducted by federal agencies (e.g., FBI, CISA, and others).

[35] See Exec. Order No. 14239, 90 *Fed. Reg.* 13,267 (Mar. 21, 2025) (signed Mar. 18, 2025), https://www.federalregister.gov/documents/2025/03/21/2025-06023/executive-order-14239-achieving-efficiency-through-state-and-local-preparedness.

c. *The provision of early warnings (i.e., the identification of cyber vulnerabilities and the assessment of countermeasures that might be available to address them).*

The NERC Electricity Information Sharing and Analysis Center (E-ISAC) provides an early warning of high severity vulnerabilities, including ones that are actively exploited in the energy sector. Additionally, CISA produces early warnings on cyber vulnerabilities for operational and enterprise technology. CISA also produces special advisory information on highly sophisticated vulnerabilities and affects many sectors beyond the energy sector (e.g., Log47 and Citrix Bleed).

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).*

The Commission should encourage the reuse of other incident reporting forms and reports in the event of an incident to avoid duplicative reporting efforts.

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).*

Like the utilities within the Commonwealth, PECO encourages the Commission to pursue close collaboration with intelligence sharing programs sponsored by the Federal government and the commercial security industry to support cybersecurity awareness and resilience in the Commonwealth.

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 Commission should share unique information that they possess with all stakeholders to ensure a complete response by industry members. If the Commission receives information

through confidential means, the Commission should work with the impacted party to ensure that information is being shared or receive authorization from the disclosing party to share the information with the affected party directly.

Question No. 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?

PECO believes that the Commission and public utilities could save administrative resources if the Commission accepts incident reports generated in response to federal cyber incident reporting regulations from those utilities subject to them. Examples of such forms are DOE-417 or CISA incident forms generated by DOE or CISA's reporting portals. PECO encourages the Commission to coordinate secure access to DOE and DHS' web portals, or absent this access, accept incident forms generated by federal portals. These incident reports will give the Commission the information it seeks with respect to cyber incidents that impact operations or customer information. PECO notes that utilities are already subject to multiple cyber incident reporting laws and expectations. PECO recommends that the Commission allow cyber incident reports generated for federal agencies to satisfy Commission cyber incident reporting requirements, where possible.

Question No. 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?

Once CIRCIA's final rule is in effect, utilities like PECO will likely be required to report substantial cyber incidents to CISA. Many of those reportable incidents to CISA would also likely trigger reporting obligations to the Commission under the ANOPR's Staff Working Proposals. Without coordination, this will result in the reporting of different information, with differing timing

requirements, to two different entities, all for the same event. However, were the Commission to adopt CIRCIA's reporting framework (once published), the failure of CISA to share its report information with the Commission would merely result in the duplication of transmission for the utilities—utilities could submit to the Commission what they are submitting to CIRCIA with minimal burden.

> *Question No. 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?*

PECO believes that the Commission can eliminate regulatory duplication/overlap by accepting compliance with federal cybersecurity regulations for those utility assets subject to those requirements and allowing alignment of remaining assets used to provide public utility service in Pennsylvania with NIST CSF, as previously discussed in Question #1. The Commission should allow utilities to demonstrate compliance through periodic self-certification and maintain sensitive compliance documents onsite subject to review. The Commission should also align with existing federal reporting requirements, formats, and timelines, ensuring efficiency while maintaining the Commission's statutory role by requesting a copy of any federally submitted incident reports rather than imposing a separate incident reporting regime.

> *Question No. 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.*

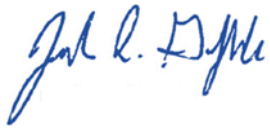
PECO does not believe that the elimination of the cybersecurity aspects in Chapter 101 of the PUC's regulations will impact the physical security, emergency response, and/or business continuity. At Exelon, Cyber and Information Security Services (CISS) and Corporate Physical Security (CPS) work together to protect digital systems and physical infrastructure to ensure the

safety, reliability, and resilience of operations based on the threat landscape. However, the removal of the cybersecurity aspects of Chapter 101 will help streamline PECO's physical security self-attestation requirement without negatively affecting this collaborative relationship to maintain secure operations.

III. CONCLUSION

PECO appreciates the opportunity the Commission has provided to offer these comments and looks forward to working with the Commission and interested stakeholders as this matter moves forward.

Respectfully submitted,



Jack R. Garfinkle (Pa. No. 81892)
PECO Energy Company
2301 Market Street
P.O. Box 8699
Philadelphia, PA 19103
E-mail: Jack.Garfinkle@exeloncorp.com

Dated July 16, 2025