Brandon J. Pierce, Esquire
Assistant General Counsel
2301 Market Street / S23-1
Philadelphia, PA 19103

Direct Dial: 215-841-4220
Brandon.Pierce@exeloncorp.com

February 8, 2023

Via E-Filing
Rosemary Chiavetta, Secretary
Pennsylvania Public Utility
Commission Commonwealth
Keystone Building
400 North Street, Second Floor
Harrisburg, PA 17120

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

Dear Secretary Chiavetta:

Attached for electronic filing please find PECO Energy Company's Comments in the above-referenced proceeding.

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

Respectfully submitted,

Brandon J. Pierce

BJP/alb
Enclosure

Cc: Colin Scott, Assistant Counsel, Law Bureau colinscott@pa.gov
Chris Van de Verg, Assistant Counsel, Law Bureau cvandeverg@pa.gov
Daniel Searfoorce, Manager (BTUS) dsearfoorc@pa.gov
Michael Holko, Director, Cybersecurity Compliance miholko@pa.gov
Karen Thorne, Law Bureau, kathorne@pa.gov

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

RULEMAKING TO REVIEW CYBER SECURITY SELF-CERTIFICATION REQUIREMENTS AND THE CRITERIA FOR CYBER ATTACK REPORTING	**:**	**DOCKET NO. L-2022-3034353**

COMMENTS OF PECO ENERGY COMPANY

On November 10, 2022, the Pennsylvania Public Utility Commission (the "Commission" or the "PUC") entered an Advance Notice of Proposed Rulemaking Order ("ANOPR") in the above-captioned docket to review its current regulations relating to cybersecurity. PECO Energy Company ("PECO" or the "Company") submits these comments in accordance with the ANOPR.

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 effective 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 comments, PECO provides responses to the Commission's questions presented in the ANOPR regarding changes to the Commission's cybersecurity regulations, potential frameworks for compliance evaluation, proposed guidelines for cybersecurity incident reporting, and regulatory harmonization with other existing and forthcoming cybersecurity requirements.

I. EXECUTIVE SUMMARY

As the Commission observed, the threat landscape facing owners and operators of critical infrastructure, particularly those in the energy sector, is rapidly evolving. As a leading electric and gas utility company, PECO understands that ensuring the security of our business is essential to continuity of service to customers in the Commonwealth and commends the Commission's interest in opportunities to improve its cybersecurity oversight program. While PECO appreciates the need to ensure that cybersecurity tools and approaches keep pace with new cyber threats, the Commission should also keep in mind that the utility industries have not been idle since the Commission's rules were first issued in 2005. Utilities across the nation, including PECO and other utilities in the Commonwealth, are constantly improving their cybersecurity programs to stay ahead of threats pursuant to federal cybersecurity requirements and advances in industry approved frameworks.

As just one example, the National Institute of Standards and Technology ("NIST") Cyber Security Framework ("CSF") has become a cornerstone of the cybersecurity program and security controls for PECO and other Exelon utilities. The NIST CSF provides an established, comprehensive, and flexible model on which PECO built its security controls program. Utilities also implement other industry standards and federal programs and have done so based on considerable evaluation and with substantial financial investments. Accordingly, PECO respectfully recommends that the Commission consider the significant progress that utilities have made to align their programs with industry standards and other federal requirements that incorporate strong cybersecurity controls and best practices.

PECO recommends that the Commission consider the following three key principles as it begins its review of the comments submitted in response to the ANOPR.

Utilities Should Be Given Flexibility to Meet Certification Requirements. PECO believes that the Commission, public utilities, and customers will be best served if public utilities have flexibility in tailoring their cybersecurity programs and strategies to their own systems. Accordingly, PECO recommends that the Commission avoid developing prescriptive requirements. Systems and operational needs are different for each utility (and type of utility), and cybersecurity principles based on an inflexible, uniform approach may hinder a utility's ability respond to the needs of its unique threat environment.

The Commission's Self-Certification Program Is Well-Suited to Provide Utilities with Flexibility. PECO believes that the Commission's existing self-certification model is sufficient to address the cybersecurity posture of public utilities in Pennsylvania because it allows those utilities to meet compliance through the development of their own cybersecurity plans. This approach offers numerous benefits, including efficiency, flexibility, and agility. Allowing utilities to leverage their experience and operating history in tailoring their cybersecurity programs preserves the Commission's administrative resources and reduces regulatory burdens for utilities, thereby allowing utilities to remain focused on providing safe, continuous, and reliable service.

Any Changes to the Regulations Should Leverage Advances Already Made by Utilities and Avoid Conflicts With, or Duplication of, Existing Standards and Requirements. Any changes to the Commission's regulations should clearly identify the Commission's security objectives and allow utilities to leverage the significant progress they have made under existing federal or higher industry standards. The Commission should not lose sight of one of its own guiding principles when designing the self-certification program—avoiding replication of regulations already in place. Whereas prescriptive requirements can create potential overlap or conflicts with other standards and regulations, flexible, outcome-based regulations will allow

public utilities to use existing tools suited to their respective environments to meet compliance without jeopardizing the Commission's oversight role.

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.

II. RESPONSE TO THE QUESTIONS PRESENTED IN THE ANOPR

> *Question No. 1: The PUC seeks 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.*

PECO believes that the Commission's existing self-certification model is sufficient to address the cybersecurity posture of public utilities in Pennsylvania. However, as discussed further in response to Question No. 3, the Commission can improve its regulations by allowing public utilities to satisfy the self-certification requirement by demonstrating compliance with existing federal or higher industry standards. PECO recommends that any proposed modifications to the Commission's existing regulations be limited to granting that flexibility. In particular, any proposed regulation by the Commission should: (1) take into account the substantial controls already implemented by utilities like PECO; (2) draw on the significant progress of, and align with, established cybersecurity frameworks; and (3) to the extent that additional controls are considered or encouraged, focus on requirements or recommendations that avoid overly prescriptive controls and instead address risk-based objectives that utilities will have the flexibility to meet through a range of industry-accepted security approaches.

It is important that the Commission carefully consider the existing substantial cybersecurity programs and investments that utilities already have in place to protect critical infrastructure in the

Commonwealth. Electric transmission systems and gas pipelines are already regulated at the federal level, and any action taken by the Commission should not conflict with those requirements. For example, Exelon utility operating companies, like PECO, have implemented enhanced controls to ensure the reliability of the bulk electric system, consistent with, or exceeding, mandatory federal requirements. Exelon also has comprehensive cybersecurity programs to protect PECO's real-time electric transmission and gas pipeline operations, consistent with the elevated risks that these systems pose, and to comply with applicable federal standards and directives. Additionally, Exelon and PECO have implemented comprehensive cybersecurity programs and controls aligned with federal and industry standards, such as the NIST CSF. These programs and controls cover and effectively secure all Exelon and PECO Information Technology ("IT") and Operational Technology ("OT") systems.

The controls and overarching programs described above reflect substantial investments by Exelon and PECO to implement cybersecurity protections for all systems that support Exelon utilities' electric, gas, and customer services operations. The Commission should consider the significant efforts that utilities, like PECO, have taken toward improving their cybersecurity posture by meeting existing mandatory requirements and aligning with generally accepted standards. Any requirements proposed by the Commission should encourage and not hinder PECO (and other critical infrastructure companies) from implementing established federal and industry security standards, like the NIST CSF. Accordingly, PECO recommends that any new requirements adopted by the Commission be limited to self-certification relating to the implementation of generally acceptable security programs.

Question No. 2: The PUC seeks comment on whether and how to update the terms and concepts used in the existing regulations to better reflect the current cybersecurity landscape, Federal and industry standards and any revisions which may be adopted in this rulemaking.

Given the numerous legal and regulatory requirements applicable to cybersecurity, there is significant potential for conflict, overlap, or duplication of terms and concepts. Accordingly, PECO urges the Commission to limit updates to those terms and concepts that are of the most interest to the Commission's security objectives.

Question No. 3: The PUC seeks comment on the relative merits and weaknesses of each of the approaches within the heading "Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities" and which of these approaches, some combination of these approaches, or some other approach, provides the PUC, the utility and its ratepayers with the greatest potential assurance that a utility is adequately prepared to address cyber security threats.

In the ANOPR, the Commission seeks comment on five potential regulatory approaches to ensure that public utilities' cybersecurity plans are adequate. These five approaches can be summarized as follows: (1) self-certification similar to the Commission's existing regulations ("Option 1"); (2) self-certification of a plan, program, or both that complies with a federal or industry standard ("Option 2"); (3) third-party expert certification ("Option 3"); (4) on-site review through management audits ("Option 4"); and (5) confidential submission of cybersecurity plans and programs ("Option 5"). PECO commends the Commission for considering this broad spectrum of options to advance its cybersecurity regulatory framework. For the reasons discussed below, ***PECO recommends that the Commission move forward with a self-certification option that combines the elements of Option 1 and Option 2***. PECO's proposed combination is addressed below, along with considerations of the relative merits and weaknesses of the other options identified by the Commission.

Option 1: Self-Certification Similar to the Commission's Existing Regulations

The self-certification approach has worked well in Pennsylvania and other states, and PECO believes that the Commission should continue to use this model as the foundation for its cybersecurity regulation. Self-certification offers numerous benefits to the Commission and regulated entities. Most notably, it is highly efficient: the self-certification approach preserves the Commission's administrative resources and alleviates regulatory burdens for utilities, thereby allowing utilities to remain focused on providing safe, continuous, and reliable service, while also providing utilities important flexibility. Owners and operators of industrial control systems, like utilities, often have highly customized or bespoke security solutions and are best positioned to tailor security controls to their own operational needs.

While PECO agrees that the Commission should continue allowing utilities to self-certify compliance, PECO also believes it is appropriate for the Commission to update its self-certification program in two ways. First, the Commission should replace the four basic security controls in its cybersecurity requirements with minimum security objectives that must be reflected in utilities' cybersecurity plans. These objectives should not be prescriptive requirements that confine the utility's compliance to a specific set of controls. Instead, the security objectives should identify at a high-level, and require utilities to mitigate through their cybersecurity plans, the areas that present the greatest operational and reliability risk. The Commission is urged to consider federal standards (*see* discussion of Option 2 *infra*) and models from other jurisdictions (*see* Question No. 5 *infra*) that implement a flexible, risk-based approach to cybersecurity compliance. Second, the Commission should account for other federal and/or industry standards in its implementation of objective-based cybersecurity requirements. On this matter, PECO refers the Commission to its comments on Option 2.

Option 2: Self-Certification Considering Federal or Industry Standards

For the reasons discussed above, PECO supports the Commission's use of the self-certification approach. However, as the Commission observed, cyber threats have proliferated considerably since the self-certification regulations were drafted in 2005. So, too, have federal and industry-led cybersecurity standards, and it is common now for utilities to balance myriad cybersecurity regulatory requirements. For example, PECO and other Exelon entities must adhere to requirements promulgated by the North American Electric Reliability Corporation ("NERC") and the Department of Homeland Security ("DHS"), including the Transportation Security Administration ("TSA"). PECO and other Exelon entities have also voluntarily built an internal Security Controls Program based on the NIST CSF. PECO respectfully submits that the Commission, like other state regulatory bodies, should avoid requirements that force utilities to duplicate the controls that they are already implementing under other programs. Specifically, PECO recommends that utilities be allowed to self-certify compliance with the Commission's security objectives through implementation of other appropriate federal or industry standards. Incorporating this feature in the self-certification program would continue to preserve one of the Commission's longstanding objectives to avoid replicating regulations that were already in place and required by the federal government or other agencies.

Option 3: Third-Party Expert Certification

PECO believes that this approach may introduce unintended risks and urges the Commission to prioritize optimization of the self-certification program. Although the use of third-party evaluators or certifiers may present some administrative efficiencies when compared to Commission evaluation, PECO believes that the Commission should weigh that benefit against the risk of inconsistencies among third party evaluations and the costs utilities will incur to implement this approach. A key factor in successful compliance programs is consistency—relying

solely on third parties to perform compliance verifications may result in divergent compliance monitoring approaches and interpretations. To avoid diverging results, the Commission would need to closely monitor third-party verification results and potentially devote additional resources to produce training and guidance for third-party verifiers. The Commission also appears to expect utilities to bear the costs of obtaining third-party verifications, which presents another burden that needs to be weighed against the potential efficiencies of this option. PECO respectfully submits that its proposal to leverage elements of Option 1 and Option 2 for a slightly modified self-certification program would provide more administrative efficiencies than the third-party proposal, all without risking the unintended consequences described above or requiring utilities to incur additional, significant, compliance costs.

Option 4: On-Site Reviews

For reasons similar to those described above in response to Option 3, PECO urges the Commission to prioritize its self-certification program. Transitioning the cybersecurity oversight program to on-site management audits will impose significant cost and resource implications for the Commission and regulated utilities alike. PECO respectfully recommends that the combination of Option 1 and Option 2 will allow the Commission to achieve its objectives more efficiently while allowing utilities to focus their resources on securing their systems instead of compliance administration. On-site reviews provide unique opportunities for utilities and regulators to share information and expectations regarding security, and PECO understands that foregoing formal on-site compliance audits may prevent the Commission and utilities from realizing that benefit. If the Commission would find it valuable, PECO stands ready to meet with the Commission and its staff

on an informational basis to answer any questions regarding its approach to cybersecurity threat mitigation and PECO's program more generally.

Option 5: Filing Confidential Copies of Cybersecurity Plans

PECO has significant concerns with this option, which would require utilities to submit their cybersecurity plans directly to the Commission for an adequacy review. Any submission of cybersecurity plans, as well as responsive comments provided by the Commission, would contain highly confidential or sensitive information related to utilities' processes and procedures, response actions, and capabilities, as well as recommended areas for improvement. Recognizing that no system is 100% secure, aggregating such sensitive information from multiple utilities can effectively provide adversaries with a single point of failure through which to gain access to security information on critical infrastructure systems, and it should be avoided to the extent practicable.

Collecting and storing highly confidential and sensitive system information in one place negates the security inherent in decentralized separate utility systems, and PECO believes the security risks outweigh any benefits in implementing this approach. There are alternative secure and transparent approaches for the Commission to review and scrutinize sensitive information (i.e., on-site documentation review or being granted access to secure company information repositories), and PECO also notes that the collection of cybersecurity plans may also present administrative challenges similar to those the Commission seeks to avoid with respect to the Self-Certification Form ("SCF") process.[1] PECO is amenable to working with the Commission to help it evaluate such approaches and help the Commission select the most secure approach. That said,

[1] *See* ANOPR at 14 ("Processing the SCF is a complex matter. . . . [T]he information contained in an SCF may constitute Confidential Security Information (CSI), which means that SCFs must be submitted on paper and filed with the Secretary's Bureau to ensure their receipt and storage comply with Pennsylvania's CSI law and the PUC's implementing regulations.").

if the Commission implements this approach, it should ensure the submission of the cybersecurity plan will not introduce additional risks due to an adversarial breach that could cause harm to a utility.

Question No. 4: The PUC welcomes comments describing the approaches taken by other state public utility commissions to address public utilities' cybersecurity fitness and evaluating their respective costs and benefits.

As explained in response to Question No. 3 above, PECO recommends that the Commission move forward with a self-certification program that is based on Commission-established security objectives and that also allows utilities to meet those objectives by demonstrating compliance with other existing cybersecurity regulatory frameworks (i.e., a combination of Option 1 and Option 2). PECO notes that other jurisdictions have already implemented such an approach. For example, the New Jersey Board of Public Utilities ("NJ BPU") requires regulated utilities to implement cybersecurity programs that address certain minimum, high-level requirements and to then submit annual self-certifications attesting to compliance with those requirements. The NJ BPU's implementing order also explicitly allows for utilities to meet their NJ BPU requirement by self-certifying compliance with an existing cybersecurity regulatory framework.[2]

In that same vein, the Maryland Public Service Commission's ("MD PSC") cybersecurity regulations identify high-level minimum requirements, while also acknowledging that utilities observe industry standards and other applicable regulatory requirements. Specifically, the MD PSC requires utilities to maintain cybersecurity plans that (1) address high-level areas of focus identified by the Commission, and (2) align with an accepted industry standard and all applicable

[2] *In the Matter of Utility Cyber Security Program Requirements*, N.J. B.P.U. Docket No. A016030196 (Mar. 18, 2016) ("In cases where Utilities have critical systems that are also subject to [NERC] Critical Infrastructure Protection ("CIP") standards, certification of compliance with those standards is sufficient to meet the annual certification requirement under this order for those critical systems. Such certification of compliance must be submitted to Reliability and Security Division Staff in accordance with the timeline noted above.").

federal and state requirements.[3] The Commission should consider adopting a similar approach under an objective-based self-certification program, which PECO proposed above.

> *Question No. 5: Would changes to the cybersecurity aspect of 52 Pa. Code § 101.3 impact the physical security, emergency response and/or business continuity aspects of the rule and/or Chapter 101 generally? The PUC seeks comment on the nature and extent of such foreseeable impacts and ways to address those impacts.*

PECO does not believe that changes to the cybersecurity aspects of 52 Pa. Code § 101.3, which preserve the Commission's self-certification program, would have any impacts on the emergency response or business continuity aspects of Chapter 101. However, if the Commission proceeds to revise its requirements in a manner that imposes prescriptive requirements or departs from the flexibility and advantages inherent to the self-certification program, PECO believes those changes could impact how utilities respond to, and manage, operational and business disruptions. Such changes could have a particularly significant ripple effect on utility companies and should be approached carefully by the Commission, with due consideration for the utility's size, operational footprint, and ability to adapt to regulatory changes. For example, drastic changes to, or a departure from, the self-certification program may present unique challenges for utility companies operating in multiple jurisdictions, like Exelon, that rely on integrated programs to implement emergency response and business continuity plans across multiple operating companies. Accordingly, PECO respectfully recommends that the Commission weigh the potential benefits of any proposed changes against the risk of interfering with utilities' ability to continue critical operational business functions that support the general public.

[3] *See* COMAR 20.06.01.03.

Question No. 8: The PUC seeks comment on ways to streamline and otherwise improve the filing, handling, and storage of SCFs.

The Commission can streamline the SCF process by eliminating the potential for the forms to contain Confidential Security Information ("CSI"), which will allow for a simplified submission process. As discussed below, PECO believes the Commission can achieve those goals without compromising its oversight role or the confidentiality of the information included in the SCF.

As the Commission noted in the ANOPR, processing the SCF can be complicated due, in part, to the possibility that SCFs may contain CSI, which is generally defined as information "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," including "[a] security plan, security procedure or risk assessment prepared specifically for the purpose of preventing or for protection against sabotage or criminal or terrorist acts."[4] The Commission can streamline its SCF submission process by ensuring that utilities do not include CSI in their SCFs.

As a preliminary matter, a utility's self-certification should not rise to the level of CSI because that information, on its own, could not be used by a threat actor to "compromise security," unless it was paired with specific information on security controls, processes, or procedures. The Commission should explicitly instruct utilities to omit such details from their SCF submissions. Furthermore, PECO's proposal to allow self-certification based on industry or federal programs will reduce the need for utilities to describe specific information because those utilities will be attesting to compliance with a broad standard.

By eliminating the likelihood that utilities will submit self-certifications containing CSI, the Commission can overcome the barrier on electronic submission, which should greatly improve

[4] 35 Pa. Stat. Ann. § 2141.2.

the administration and processing of SCFs. To be clear, PECO is proposing to streamline the self-certification process but continues to believe that the SCFs should still be handled securely by both the Commission and the submitting utility. Accordingly, PECO recommends that the Commission allow electronic submission of SCFs without CSI through a secure, encrypted file transfer mechanism (e.g., secure File Transfer Protocol), which will continue to provide confidentiality and data security protections while alleviating some of the administrative burdens that exist today.

> *Question No. 9: The PUC seeks comment on whether and how to streamline the self-certification form, plan and reporting requirements to better calibrate the benefits of the existing regulations against the burdens they place on regulated entities, especially smaller utilities, and on PUC staff.*

PECO's recommendations in these comments regarding the self-certification program, the SCF submission process, and the Commission's reporting requirements seek to balance efficiency and flexibility with the Commission's security and oversight objectives. As discussed above, PECO believes the self-certification program works well in Pennsylvania and recommends that the Commission not deviate from this approach to cybersecurity compliance. To the extent the Commission considers applying its regulations "in a granular manner,"[5] PECO recommends that the Commission do so using an industry standard risk-based approach. For example, the Commission could conduct a risk-based assessment to determine which entities may have lower regulatory burdens based on their lower risk profile relative to other regulated utilities.

> *Question No. 10: The PUC seeks comment on potential ways to revise the reporting criteria in its existing regulations, including the potential addition of new requirements for reporting incidents involving IT.*

PECO believes that to be effective, cyber incident reporting regulations must (1) define a clear reporting threshold based on the potential impact to the utility's own IT and/or OT environments, and (2) balance the regulator's need to receive timely incident information against

[5] ANOPR at 15.

the reporting burden on the utility. Thus, if the Commission opts to modify its existing regulations, PECO recommends that it first establish a minimum threshold ***that is tailored to the specific risks that the Commission hopes to mitigate with utility-supplied incident information***. The reporting threshold should generate useful potential threat information for the Commission while avoiding complicating utility incident response activities with expansive and burdensome requirements.

PECO believes that useful threat information captures confirmed cyber incidents, and not simply potentially suspicious "noise" that did not pose a material risk. An overly broad threshold that forces the utility to report on unconfirmed incidents could inundate the Commission with low-impact-level data resulting from cyber-related events that pose no risk to customers or the secure and reliable delivery of utility services. Thus, the Commission should avoid regulations that would overwhelm and flood the Commission with unusable data, and that would tie up limited utility security resources in reporting and coordinating on minor events. Instead, the Commission should focus on fostering an efficient, effective, and collaborative reporting program, with an emphasis on realistic, impact-based thresholds and achievable reporting goals. With respect to IT systems, reporting should only be triggered when there is an actual compromise of real-time systems or customer information, and reporting on OT system incidents should be designed to promote safety, transparency, and accountability, while protecting the reporting utility's identity.

Question No. 11: The PUC seeks comment with respect to the continuing efficacy of the $50,000 reporting threshold.

PECO recommends that the Commission revise its regulations to transition the existing monetary reporting threshold to an impact-based threshold. As noted above, PECO believes that a reporting threshold should be designed to generate useful potential threat information for the Commission and avoid inundating the Commission with relatively minor incident data or data that is ultimately determined to be irrelevant.

The Commission appears to have set the $50,000 threshold to avoid reporting of minor events and to capture data related to incidents "that result in a significant expense."[6] PECO respectfully recommends that a dollar-based threshold is not necessarily probative. As a practical matter, attributing a dollar value to the impact of a particular cybersecurity incident can be incredibly difficult or even impossible. Moreover, utility resources would be better spent focusing on incident response remediation and restoration efforts as opposed to calculating administrative thresholds. Instead, requiring reporting based on a cybersecurity event that has been confirmed by the utility to have materially disrupted or caused degradation of systems, impacted critical infrastructure, or business operations is far a more substantive and actionable threshold for reporting purposes.

> *Question No. 13: The PUC seeks comment on the potential for conflict, overlap, redundancy, or other bases warranting review in the interplay between the PUC's cybersecurity regulations (and revisions thereto) and Federal initiatives, including but not limited to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).*

PECO supports the Commission considering ways in which it may reduce the potential for regulatory duplication, overlap, and conflicts with other regulations and initiatives. In particular, the Commission should reduce the potential for regulatory conflicts and redundancy by focusing on objective-based regulations rather than imposing prescriptive requirements. Whereas prescriptive requirements can create potential overlap or conflicts with other regulatory requirements, objective-based regulations will satisfy the Commission's security objectives while allowing utilities to leverage existing tools suited to their respective environments to meet compliance. Thus, as explained in response to Question No. 3, the Commission should consider

[6] Final Rulemaking Order, *Proposed Rulemaking for Revision of 52 Pa. Code Chapters 57, 59, 65 and 67 Pertaining to Utilities' Service Outage Response and Restoration Practices*, Pa. P.U.C. Docket No. L-2009-2104274 (order entered Sept. 23, 2011) at 10 (Jan. 7, 2012).

revising its program to identify minimum security objectives and allowing utilities to meet those objectives by applying controls from comparable cybersecurity regulations.

With respect to incident reporting, PECO notes that utilities are already subject to multiple cyber incident reporting laws or expectations. In the energy sector, for example, TSA's Security Directive Pipeline-2021-01B requires reporting within 24-hours "as soon as an incident is identified and requires entities to develop a Cybersecurity Incident Response Plan to mitigate operational risk and disruptions,"[7] and NERC requires reporting "one hour within determination of a reportable incident."[8] Meanwhile, as the Commission observed in the ANOPR, the DHS's Cybersecurity and Infrastructure Security Agency is promulgating cyber incident reporting rules pursuant to CIRCIA, which will require critical infrastructure entities to report covered cybersecurity incidents within 72 hours from the time the entity reasonably believes the incident occurred and ransomware payments within 24 hours.[9] To the extent the Commission seeks to revise its cybersecurity incident reporting requirements, PECO recommends that the Commission consider the interplay between its proposed regulations and the existing and forthcoming incident response regulations described above to limit the burden on utilities caused by duplicative or conflicting reporting requirements. PECO notes that pursuant to CIRCIA, DHS has been tasked with establishing a Cyber Incident Reporting Council composed of federal agencies that will coordinate, deconflict, and harmonize existing and future federal cyber incident reporting requirements. PECO offers this initiative for the Commission's consideration as an example of

[7] *See* Transportation Security Admin., Security Directive Pipeline-2021-01B (May 29, 2022): https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf.

[8] *See* NERC Reliability Standard CIP-008-6.

[9] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (6 U.S.C. §§ 681, *et seq.*)

how regulatory bodies can improve cybersecurity regulation through inter-agency coordination, all while reducing the burden of duplicative or conflicting requirements on industry.

> *Question No. 12: The PUC seeks comment on the pros and cons of merging the self-certification and cyber incident reporting regulations into a single chapter of the Code, and otherwise eliminating unintended or unjustified inconsistencies in the existing regulations.*

PECO does not oppose combining the self-certification and cyber incident reporting requirements into a single chapter of the Code. Utility self-certification under the Commission's cybersecurity program and the cyber incident reporting requirements are interrelated topics, and it is reasonable for those provisions to be centralized for ease of reference. If the Commission chooses to make these changes, it should harmonize the terminology within those sections and, to the extent needed, eliminate unintended or unjustified inconsistencies in the existing regulations.

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,

Anthony E. Gay (Pa. No. 74624)
Jack R. Garfinkle (Pa. No. 81892)
Brandon J. Pierce (Pa. No. 307665)
PECO Energy Company
2301 Market Street
P.O. Box 8699
Philadelphia, PA 19103
E-mail: Brandon.Pierce@exeloncorp.com
Jack.Garfinkle@exeloncorp.com

Dated: February 8, 2023

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 attached 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

Richard Kanaskie
Director & Chief Prosecutor
Bureau of Investigation and Enforcement
Commonwealth Keystone Building
400 North Street, 2nd Floor West
PO Box 3265
Harrisburg, PA 17105-3265
rkanaskie@pa.gov

Candis A. Tunilo
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
ra-sba@pa.gov
tereswagne@pa.gov

Donna M.J. Clark
Vice President & General Counsel
Energy Association of PA
800 N. Third Street, Suite 205
Harrisburg, PA 17102-2025
dclark@energypa.org
nluciano@energypa.org

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

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

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

Pamela C. Polacek
CT Enterprises, Inc.
1775 Industrial Blvd.
Lewisburg, PA 17837
ppolacek@ctenterprises.org

Kimberly A. Klock
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
Duquesne Light Company
411 Seventh Avenue, MailDrop 15-7
Pittsburgh, PA 15219
lbaxter@duqlight.com

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

Dated: February 8, 2023

Brandon J. Pierce (Pa Attorney No. 307665)
Counsel for PECO Energy Company
2301 Market Street, 23rd Floor
Philadelphia, PA 19103
(215) 841-4220
Brandon.Pierce@exeloncorp.com