

Darsh Singh, Esq.  
(610) 212-8331  
(330) 315-9263 (Fax)

February 8, 2023

**VIA ELECTRONIC FILING**

Rosemary Chiavetta, Secretary  
Pennsylvania Public Utility Commission  
Commonwealth Keystone Building  
400 North Street, 2<sup>nd</sup> 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:

Pursuant to the Pennsylvania Public Utility Commission's Advance Notice of Proposed Rulemaking Order entered on November 10, 2022 in the above-captioned proceeding, enclosed herewith for filing are the Comments of Metropolitan Edison Company, Pennsylvania Electric Company, Pennsylvania Power Company and West Penn Power Company.

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

Very truly yours,



Darsh Singh

DS/dml

Enclosures

c: As Per Certificate of Service

**BEFORE THE  
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

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

---

**COMMENTS OF METROPOLITAN EDISON COMPANY,  
PENNSYLVANIA ELECTRIC COMPANY, PENNSYLVANIA POWER  
COMPANY AND WEST PENN POWER COMPANY**

---

**I. INTRODUCTION**

On November 10, 2022 the Pennsylvania Public Utility Commission (“PaPUC” or “Commission” or “PUC”) entered the Advance Notice of Proposed Rulemaking Order (“ANOPR”) to review its current regulations relating to cybersecurity, which was subsequently published in the Pennsylvania Bulletin on December 10, 2022 under Docket No. L-2022-3034353. The PaPUC 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 ANOPR, Metropolitan Edison Company (“Met-Ed”), Pennsylvania Electric Company (“Penelec”), Pennsylvania Power Company (“Penn Power”), and West Penn Power Company (“West Penn”) (each of which may be referred to as “Company” and/or in combination as “Companies”) respectfully submit the following response within 60 days of the ANOPR’s December 10 publication in the Pennsylvania Bulletin.

## II. BACKGROUND

The Companies commend the PaPUC for recognizing the quickly evolving cybersecurity landscape and the importance of maintaining robust public utility cybersecurity fitness. Given the ever-shifting threat vectors, the Companies fully support the Commission's efforts to review regulations relating to cyber attack reporting and self-certification. While the Companies generally believe that the existing regulations regarding cyber attack reporting and self-certification *do not* need to be revised, to the extent that the Commission does make any modifications, the Companies submit these comments for consideration.

The Commission must strike a delicate balance – cyber 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. Further, ambiguous definitions and regulations cannot be implemented with any certainty or efficiency. On the other hand, overly granular regulations will force jurisdictional utilities to expend resources to comply with regulations that may not align with their existing operating systems. As such, throughout the comments herein the Companies urge the Commission to consider a “result-based” approach which more closely tracks with the definitions and language of cyber reporting requirements set by the North American Electric Reliability Corporation (“NERC”) and cyber incident reporting federal guidance.<sup>1</sup> As aptly noted in the ANOPR, a result-based approach “do[es] not specify a technology or method to achieve compliance, rather leaving it up to the utility to decide how best to comply with the standards.”

---

<sup>1</sup> See Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government, *available at* <https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf> (last visited October 21, 2021).

These comments address the Topics for Comment in Appendix A of the ANOPR in the order they are raised. For ease of reference, the Topics for Comment are restated prior to the Companies' responses to each.

### **III. COMMENTS**

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. *See ANOPR at 2.*

#### **Comments:**

The Companies prioritize cybersecurity and, as shown through their robust cybersecurity program, comply with all state, federal, and local reporting requirements. Both when creating their cyber program, and when revisiting the program on a consistent basis to ensure it withstands constantly evolving threats to utilities, the Companies utilize a myriad of resources, guidance, regulations, protocols and best practices. Meaning, the Companies do not rely solely on state public utility commission regulations to guide their cyber fitness. As such, the Companies find the existing regulations to be sufficient and *do not* require revisions as they currently work well to compliment all the existing standards and guidance. In fact, the Companies caution the Commission from unnecessarily complicating an already crowded regulatory landscape that may lead to conflicting messaging to utilities. There are already several entities and agencies with their “hat” in the cyber regulatory “ring,” including but not limited to: NERC with its Critical Infrastructure Protection (“CIP”) Standards, the National Institute for Standards and Technology

(“NIST”), the Federal Energy Regulatory Commission (“FERC”), and the Cybersecurity and Infrastructure Security Agency (“CISA”)<sup>2</sup>.

### **A. Updating Terms and Concepts**

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. *See* ANOPR at 9.

#### **Comments:**

The Companies support defining terms around cybersecurity in ways that stand apart from incident reporting, but also caution against adopting a general term that is used to encompass a wide variety of industries to the neglect of the unique needs of a utility company. While the use of “CIA Triad,” cited in the ANOPR, can be helpful in understanding risk exposure and threat severity to an individual system, each determination of “confidentiality, integrity, and availability” per the CIA Triad will be unique across each utility and no two will align in implementation; this will lead to confusion or unworkable standards. Similarly, NIST frameworks and standards are intended to serve as a good starting point for implementation of a customized security program; however, adopting one or more of the NIST standards or frameworks wholesale will lead to the inconsistent application of regulations as utilities attempt to interpret broad language and then transpose them to their specific systems and operations.

For example, to effectively use NIST standards such as the NIST Cyber Security Framework (“CSF”) or NIST 800-53, each company must take the text of the standard, interpret the standard’s language such that it can be applied to their industry and situation, and then develop a cyber security program or map internal specifications back into an existing cyber program.

---

<sup>2</sup> While not mentioned in the ANOPR or further in these comments, CISA provides guidance and support for the entire critical infrastructure sector, including the electric sector, and its guidance applies to distribution level utilities.

Ultimately, each company maintains a unique cyber security program based on its unique interpretation of the relevant NIST standards. Such variance in utility cyber security programs leaves ambiguity for consistent execution and would make regulatory oversight nearly impossible. Furthermore, defining broad terms such as “cyber risk” is also potentially unhelpful simply because the landscape of risk is constantly evolving and changing, and a workable definition will by necessity be generic and high level.

Instead of conforming to non-industry specific standards, the Companies suggest focusing on information and definitions to drive reporting of information that is of most interest and actionable by the PaPUC. Definitions and reporting should be centered around service interruptions, failures to deliver service by the utilities, or the theft and misuse of Commonwealth residents’ information. This results-based approach focuses less on the individual process or operations that each utility has in place but rather allows the Commission to ultimately obtain the information that is most pertinent to it. To that end, the Companies recommend the following definitions to align with other federal and state regulations, to speak directly to the needs of utilities, and to prevent an overload of unnecessary and expensive reporting that must be processed by both the utilities and the PaPUC:

*Utility Computer System* – 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.

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

*Cyber Security 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 a system;
2. An otherwise-authorized user exceeding authorized levels of access; or

3. Malicious exposure of data protected specified in Pa. Cons. Statues., Title. 73, Ch. 43 §§ 2301 - 2308

*Reportable Cyber Security Incident* – A Cyber Security Incident that has impacted a Utility Computer System and resulted in a failure to deliver utility services to customers or resulted in confirmed theft of protected data of utility customers.

Having tailored and targeted definitions will help utilities properly focus and align resources for maximum effectiveness and not subject the PUC to unnecessary reporting, questions, and interpretation confusion. Lastly, it should be noted that the above language tracks the definitions that were adopted by New Jersey in a recent rulemaking proceeding.<sup>3</sup> For the reasons listed in Section B.4, maintaining standards consistent with adjacent jurisdictions creates efficiencies for entities that operate across multiple jurisdictions.

## **B. Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities**

The Companies applaud the Commission for reevaluating its existing security controls under 52 Pa. Code § 101.4 and considering the other existing frameworks in light of the continuously evolving threats detailed in the ANOPR such as ransomware and attacks on public utilities’ operational technology (“OT”). Finding the correct approach is a difficult balancing act and is no easy task. Here again, the Companies urge 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. The ANOPR correctly notes that a result-based approach “do[es] not specify a technology or method to achieve compliance, rather leaving it up to the utility to decide how best to comply with the standards.”

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

---

<sup>3</sup> Definitions similar to those proposed here were adopted in 54 N.J.R. 1612(a). *See generally In the Matter of the Proposed Readoption with Substantial Amendments to N.J.A.C. 14:3, et seq.*; Docket No. AX21070998.

assurance that a utility is adequately prepared to address cyber security threats. *See* ANOPR at 13.

**Comments:**

The Companies have listed each of the bullet-point approaches in the ANOPR below and addressed each in the order in which they appear:

- Similar to the existing regulations, require a public utility to self-certify that it has a plan, a program, or both, that complies with criteria set forth in the PUC’s regulations and to report annually to the PUC that such plans and/or programs exist and are updated and tested annually.

The Companies strongly suggest that the Commission continue to require self-certification similar or the same as that in the existing regulations. These annual reports ensure that, at least once a year, jurisdictional utilities are evaluating their cybersecurity plans to ensure continued compliance and to performing any necessary updates. Any new self-certification process, similar to the one in place, should align directly with the needs and objectives of the PaPUC 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 and provides a vehicle for addressing utility deficiencies in a reasonable manner without substantially increasing the regulatory burdens and costs unnecessarily.

- Require a public utility to self-certify that it has a plan, a program, or both, that complies with an appropriate Federal or industry standard and to report annually to the PUC that such plans and/or programs exist and are updated and tested annually

In order to fully respond to this proposed approach, the Companies respectfully seek clarification as to which “Federal or industry standard[s]” the PUC had in mind to require self-certification to and the type of certification that would be requested. To the extent that the ANOPR is seeking self-certification of other federal standards such as the NIST CSF, the Companies



reference their earlier comments regarding implementation considerations. The Companies already incorporate guidance from such diverse sets of NIST guidelines in their cyber security program and operations including examples such as NIST 800-54, NIST 800-82, NIST 800-88, and NIST 800-131. To further mature the cyber program, the Companies are already aligning under the NIST CSF to track ongoing maturity in cyber disciplines. However, such implementations are necessarily customized cyber security programs and not per se implementations of a NIST standard itself. It would be difficult to credibly attest to self-certification of a standards framework that by design is customized during each specific implementation subject to diverse organizational needs. Self-attestation to a NIST framework or standard would, ultimately, be a self-attestation of a customized security program as contemplated in the approach preceding this one. The Companies value the flexibility of being able to select from the collection of NIST guidance and apply it to specific situations or needs while not being forced to implement certain elements that may not have relevance to a particular company or situation.

To the extent that this is suggesting that Pennsylvania's jurisdictional entities self-certify that they are compliant with existing NERC CIP Standards, as they apply to the bulk power system affecting Pennsylvania, the Companies are supportive of such an approach. The Companies have a robust cybersecurity program that complies with all federal and industry standards. Ensuring compliance with existing NERC CIP Standards through self-certification has all the same benefits mentioned above pertaining to an annual self-check as a way to proactively adjust for deficiencies. In fact, FirstEnergy's<sup>4</sup> wholly owned New Jersey subsidiary, Jersey Central Power & Light ("JCP&L"), already self-certifies NERC CIP compliance for the New Jersey Board of Public

---

<sup>4</sup> The Companies are wholly owned subsidiaries of FirstEnergy Corp. ("FirstEnergy") which has a footprint that spreads across six states: Ohio, Pennsylvania, New Jersey, New York, West Virginia and Maryland.

Utilities. New Jersey requires self-certification on an annual basis which includes attestation that the bulk electric system affecting NJ operations is compliant with NERC CIP as part of NJ BPU order AO16030196.

However, if the ANOPR is suggesting that jurisdictional utilities somehow certify that their distribution-level assets comply with NERC CIP Standards (which the CIP Standards are not intended for) then the Companies strongly oppose this as simply not feasible. As the ANOPR correctly states, NERC's CIP Standards are currently applicable to the bulk power system and *not* to distribution-level assets. Compliance with NERC CIP is a resource-intensive undertaking designed to protect certain types of large-impact assets within the bulk electric system. As it relates to the Companies' delivery of electric service to consumers on the distribution level, the NERC CIP standards would be unnecessarily complex and burdensome relative to the protection needs of distribution-level electric utility service within the Commonwealth. Notably, NERC CIP Standards differentiate between "high" "medium" and "low" impact assets because they acknowledge that the same level of regulation is not required for assets that are not large-impact (such as most distribution-level assets). Should the PUC attempt to implement CIP-like requirements on distribution-level assets, utilities would require significant operations and maintenance ("O&M") rate recovery increases for quickly diminishing benefits outside of the level of bulk electric system transmission.

- Require a public utility to provide a third-party expert certification that the public utility has a plan, a program, or both, in place that comply with a relevant Federal or industry standard appropriate to that utility and to report annually to the PUC that such plans and/or programs exist and are updated and tested annually.

While it is unclear which Federal or industry standards the ANOPR is contemplating, in looking at existing federal standards, there is no one-sized-fits-all standard by which a utility could be objectively measured, nor would such a standard be in the best interests of furthering cost-

effective and efficient cyber security. Often, imposition of an overly broad or insufficiently targeted standard results in cyber security resources being allocated towards compliance with a standard rather than actual system protections. As outlined in the comments for the preceding option, each implementation is necessarily customized and would require significant resource investment to engage in a third- party audit leading to a certification. Further, it is unclear what a third-party expert certification would accomplish that a self-certification of compliance could not.

Furthermore, in considering a third-party certification process, the Commission should evaluate what is already reviewed through PaPUC management audits or via other, already built-in, processes. As the Commission is well aware, the Companies are subject to intensive audits which cover a wide range of Company operations including cybersecurity. In the Companies' most recent management audit, a large number of data requests were sought and interviews were conducted on all facets of the Companies' security plans and operations, including budgeting, planning, execution, and incident response activities. This audit also covered the integration of security functions into information technology ("IT") and OT environments. Further, to the extent that the ANOPR is suggesting a third-party expert certify compliance with NERC CIP requirements as they apply to bulk electric assets, this function is already squarely covered by the Companies' Regional Entity, ReliabilityFirst. In sum, it is unclear what federal or industry standards a third-party could be brought in to evaluate and there are already checks in place to verify compliance with respect to many of the items the PUC may be concerned with.

- Integrate an onsite review of cybersecurity measures, plans, and programs into the PUC's public utility management audit process and examine cybersecurity measures, plans, and programs in place as a part of the management audit function.

Requiring PUC onsite review of plans during management audits is possible. However, cyber security plans are often complex and auditors performing management audits may not be in

the best position to interpret and evaluate plans without broader knowledge and experience within a particular utility. The Companies would be concerned that executing a cyber assessment during a management audit could lead to excessive cycles of audit examinations and clarifications without adding significant security or oversight value.

- Require a public utility to file a confidential copy of its cybersecurity plans and programs with the PUC and enable the PUC to directly review and comment on the adequacy of such plans and programs and, where deficiencies exist, require conformance with regulatory standards

As mentioned in detail above, PaPUC management audits already enable the PUC to gather relevant information regarding the Companies' cybersecurity plans and programs. During the audit, the Companies discussed their cyber programs extensively with PUC Staff. Further, given the sensitivity of cybersecurity programs and the details within them, the Companies have historically declined to provide detailed program documents to any external party, including state utility commissions.

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. See ANOPR at 13.

**Comments:**

FirstEnergy and its subsidiaries are often active participants in state utility commission cybersecurity proceedings in these other states and thus have extensive experience with other state utility commissions regarding public utility cybersecurity fitness and associated cost-benefit analysis undertaken in other jurisdictions. Consistent with the positions taken by FirstEnergy and its subsidiaries in those proceedings, the Companies advocate that state utility commissions hold its jurisdictional utilities reasonably accountable for cybersecurity without creating undue burden.

The definitions and approaches proposed in these comments are very similar to what the Companies have proposed in other jurisdictions or were adopted in those states.

At a high level, Maryland has promulgated Code of Maryland Regulations (“COMAR”) Title 20, Subtitle 06 which defines “good cyber security practice.”<sup>5</sup> and requires that, at a minimum, cybersecurity plans shall address cybersecurity-related governance, risk management, procurement practices, personnel hiring, training policies, situational awareness, response, recovery, and transparent reporting of cybersecurity incidents to State and federal entities. Additionally, COMAR 20.06.01.04 and COMAR 20.06.01.05 specify certain cybersecurity periodic reporting and breach reporting, respectively. Similarly, in New Jersey under the NJ Board of Public Utilities order A016030196, JCP&L has a self-certification process for cyber security risks similar to considerations already in place in Pennsylvania and contemplated elsewhere in these comments. Additionally, New Jersey Administrative Code (“N.J.A.C.”), Title 14 Chapter 3 has recently enhanced requirements for transparent reporting of cyber security incidents to the state.

Given the feedback above, there are several reasons why the PaPUC should strongly consider adopting an approach and definitions consistent with the public utility commissions in surrounding states:

- Consistency across regions: Having consistent cybersecurity fitness requirements across neighboring states can ensure that utilities operating in those states are held to similar standards, which can help to reduce the risk of security breaches and ensure continuity of service in case of an incident.

---

<sup>5</sup> COMAR 20.06.01

- Economies of scale: Utilizing similar regulations across states can make it easier for utilities to comply with regulations and can also allow for more efficient use of resources, such as staff and technology. Utilities will have the ability to effectively marshal and target resources across a common set of criteria.
- Interconnectedness of the grid: The electric grid is interconnected across states, having consistent cybersecurity regulations can help protect the entire grid from cyber threats, which can be more effective than having different regulations in each state.
- Regional Threats: Having consistent approaches across neighboring states can also help to address regional cyber threats that may affect multiple states.
- Compliance and enforcement: Consistent regulations can simplify compliance and enforcement efforts for both utilities and regulatory agencies.
- Best Practices: Consistency across neighboring states can help ensure that utilities are following industry best practices and standards, which can help ensure that they are well-prepared to address cyber threats.

Overall, having a consistent cybersecurity fitness approach across neighboring states can help ensure the safety and security of the electric grid and the continuity of service for customers. It can also help utilities and regulatory agencies to more efficiently use resources and address regional cyber threats.

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. See ANOPR at 13.

**Comments:**

It is difficult for the Companies to comment on the impacts the changes would have to physical security, emergency response and/or business continuity aspects of the rule or Chapter 101 without seeing the proposed changes. Generally speaking, any changes that are overly prescriptive which require adjustments to current plans, protocol, operations or systems will have a ripple effect as the Companies work to implement them. As written, the Companies do not see a need for changes to the existing requirements in 52 Pa. Code § 101.3. The Companies are compliant with the current requirements and do not find them overly burdensome. Again, to the extent that the PaPUC is considering changes to Chapter 101, the Companies urge the Commission to focus on an approach that is results and outcome-focused rather than attempting to apply granular requirements that may lead to unnecessary resources being expended to implement requirements that will not be equally beneficial to all jurisdictional utilities because of their different systems, operations and cyber maturity.

6. The PUC seeks comment on whether the self-certification regulations should be applied to additional types of entities that are subject to the PUC’s supervision? See ANOPR at 13.

**Comments:**

The market continues to trend in a direction which requires jurisdictional entities to share potentially sensitive information with various entities to offer electricity savings, usage management, demand response-programs and sustainability goals. While those defined as “jurisdictional entities” under 52 Pa. Code § 101.2 are required to submit a Self-Certification Form (“SCF”), the entities with whom sensitive data is exchanged are often not required to certify any type of cyber fitness by the Commission. For these reasons, the Companies suggest that the

Commission consider self-certification requirements for the various entities that are players in today's market.

7. The PUC seeks comment as to whether there are public utility types which should be wholly or partially exempt from the self-certification, based on easing the regulatory burden on small businesses, or for other reasons. See ANOPR at 14.

**Comments:**

The Company has no comment on this other than the considerations detailed directly above.

**C. Improving the Self-Certification Form (“SCF”) Process**

8. The PUC seeks comment on ways to streamline and otherwise improve the filing, handling, and storage of SCFs. See ANOPR at 15.

**Comments:**

The Companies are unable to comment on ways to streamline or improve the process because the Companies do not have any of the confidentiality issues described in the ANOPR. The Companies find the current SCF process to be straightforward and are not aware of an instance in which any Confidential Security Information has had to be filed as part of its SCF. Due to the lack of confidential information, there has been no need to submit on paper and file with the Secretary's Bureau. Thus, the filing, handling and storage issues detailed by the ANOPR are not applicable to the Companies or the SCF submitted by the Companies each year.

It should be noted, however, that the actual process for dissemination of the form is something that the Companies believe could be improved upon. The Secretary of the PUC sends a letter to the main company contact on file with the PUC but the letter does not successfully make it to the Companies' Regulatory Reporting team despite the Companies' Regulatory Reporting



team having been put on the distribution list several years ago. Therefore, the due date of the SCF is never clear to the Companies.

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. See ANOPR at 15-16.

**Comments:**

The Companies do not find the current self-certification requirements burdensome and, as stated above, strongly recommend the current self-certification comments be continued. While the Companies cannot speak to the burdens placed on smaller utilities, the Companies understand that self-certification is implicitly tied to the particular regulations that entities are required to affirm they comply with. Should regulations and definitions (like those proposed above) follow a “result-based” approach, as suggested by the Companies, all utilities regardless of size can be held to a standard based on the desired outcome rather than focusing on the methodology used to arrive there. This would be a more effective approach since a utilities’ methodology would greatly vary based on company size, resources, cyber-maturity and expertise.

**D. Updating Cyber Attack Reporting Regulations**

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. See ANOPR at 17.

**Comments:**

To be effective, such 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. The current reporting requirement, as written, takes the result-based approach – meaning, it requires reporting when a cyber attack leads to an interruption of service or \$50,000 in damages. Should the Commission seek an alternative but similarly result-based approach to cyber incident reporting, the Commission should consider the definition of Cyber Security Incident proposed in response to ANOPR #2 above.

The Companies have no proposed changes to the reporting requirements as written except to note that current requirement states the need to “immediately” report cyber security incidents which may not be consistent with the realities of a cyber incident. “Immediately” is somewhat vague and not always feasible. While it may be clear when an interruption of service occurs, sometimes it takes time to assess the monetary value of damages that occur. Cyber incidents are often complex and the extent of damage/exposure is not always immediately clear.

If the PUC seeks to add potential requirements for reporting incidents involving IT, the PUC should be careful not adopt regulations requiring reports of “attempted compromises” of Utility Computer Systems as has been done in other states and at the NERC CIP level. Reporting “attempted” compromises requires a significant level of subjectivity in determining intent, potential impact, likelihood, etc. that results in an uneven reporting landscape. It also requires significant internal resource investment to track and analyze various telemetry sources to find things that may require reporting. The Companies view industry collaboration, through information sharing to the Electricity Information Sharing and Analysis Center (“E-ISAC”), to be a much better process and a more efficient use of resources. The Companies suggest that the PUC form a relationship with the various existing information communities for awareness and partnership rather than requiring regulatory-based information sharing, thus creating duplicative efforts for jurisdictional utilities.

11. The PUC seeks comment with respect to the continuing efficacy of the \$50,000 reporting threshold. See ANOPR at 17.

**Comments:**

The Companies question the efficacy and efficiency of placing any monetary threshold on cyber reporting. First, the number \$50,000 feels arbitrary. There is no reason to believe that \$50,000 is the cut off for what is considered a significant cyber incident versus a non-consequential one. Second, as pointed out above, many times it is not immediately clear what the monetary impact of a cyber incident is and making this type of assessment is not only ambiguous but leads to wasted time, energy and resources to determine the monetary damage. A result-based approach which focuses on the *outcome* that the Commission is concerned about, is far more valuable of a benchmark. This will more likely give the Commission the types of reports they seek as well as be simpler for a utility to execute. With this in mind, the Companies have proposed a definition of “*Cyber Security Incident*” that focuses on triggers that the PaPUC is likely concerned with: (1) a breach or degradation of the confidentiality, integrity, or availability of a system; (2) an otherwise-authorized user exceeding authorized levels of access; or (3) malicious exposure of data protected by and specified in Pa. Cons. Statutes, Title. 73, Ch. 43 §§ 2301 – 2308. Lastly taking this result-based approach would be consistent with the approaches taken in New Jersey and Maryland.

**E. Merging the Self-Certification and Cyber Attack Reporting Regulations**

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. See ANOPR at 18.

**Comments:**

The Companies generally support modifications that aim to streamline regulatory language in a manner that simplifies, eliminates ambiguity and removes any inconsistency. In this particular

case, the Companies cannot comment specifically on the pros and cons of merging the self-certification and cyber incident revisions without seeing the language in the proposed merged provisions.

#### **F. Cost-Benefit Analysis**

13. The PUC seeks comment on how best to justify revisions to the existing regulations under the Regulatory Review Act standards. In particular, the PUC seeks comment on how the costs and benefits associated with its existing regulations, and any revisions thereto, can be objectively quantified and evaluated. *See* ANOPR at 19.

#### **Comments:**

Given the Companies' overall position that there is no need for changes to the existing regulations, a cost benefit analysis to justify revisions to the regulations is something that the Companies do not have a position on. However, should the Commission decide to implement changes to the reporting requirements or include additional benchmarks for self-certification and those changes result in an increased cost of compliance for the Companies, the Companies urge the PUC to take this into account when setting rates for jurisdictional utilities. Additional cybersecurity requirements will result in higher O&M costs, all of which must be recoverable through a utility's rate base.

#### **G. Eliminating Regulatory Duplication and Overlap**

14. 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 (CIRCA). *See* ANOPR at 21.

#### **Comments:**

Please reference the Companies' response to ANOPR #1 where the concerns with a "crowded" regulatory cybersecurity arena were addressed. Adding to this already saturated

regulatory space could lead to conflicting regulations, confusion and unintentional non-compliance as utilities struggle to grapple with the various sources of guidance and regulations in this area. In reference to CIRCIA specifically, the Companies would only urge the PaPUC not to “pile on” to what is already covered by CIRCIA or duplicate those efforts in any way.

## **H. Other Matters**

15. Finally, the PUC seeks comments as to any additional considerations that parties may wish to raise at this time relating to PUC oversight and regulation of public utilities and licensed entities as it relates to their cybersecurity fitness. *See ANOPR at 21.*

### **Comments:**

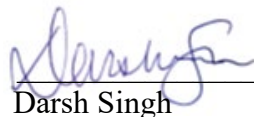
The Companies do not have further commentary.

#### IV. CONCLUSION

Metropolitan Edison Company, Pennsylvania Electric Company, Pennsylvania Power Company and West Penn Power Company appreciate the Commission's opportunity to provide comments in response to the Secretarial Letter, and the advancement of this proceeding. The Companies look forward to further collaboration and discussion with the Commission and interested stakeholders on this important topic.

Respectfully submitted,

Dated: February 8, 2023



---

Darsh Singh  
Attorney No. 330971  
FirstEnergy Service Company  
2800 Pottsville Pike  
P.O. Box 16001  
Reading, PA 19612-6001  
(610) 212-8331  
[singhd@firstenergycorp.com](mailto:singhd@firstenergycorp.com)

*Counsel for Metropolitan Edison Company,  
Pennsylvania Electric Company, Pennsylvania  
Power Company and West Penn Power Company*

**BEFORE THE  
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

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

**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 as follows:

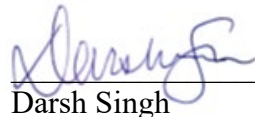
NazAarah Sabree  
Office of Small Business Advocate  
555 Walnut Street  
Forum Place, 1st Floor  
Harrisburg, PA 17101  
[ra-sba@pa.gov](mailto:ra-sba@pa.gov)  
[tereswagne@pa.gov](mailto:tereswagne@pa.gov)

Richard Kanaskie, Esquire  
Bureau of Investigation & Enforcement  
Commonwealth Keystone Building  
400 North Street, 2nd Floor West  
Harrisburg, PA 17105-3265  
[rkanaskie@pa.gov](mailto:rkanaskie@pa.gov)

Patrick M. Cicero, Esquire  
Office of Consumer Advocate  
555 Walnut Street, 5<sup>th</sup> Floor  
Forum Place  
Harrisburg, PA 17101  
[pcicero@paoca.org](mailto:pcicero@paoca.org)

Patti Kay Wisniewski  
Regulatory Agent  
1600 JFK Boulevard  
4 Penn Center  
Philadelphia, PA 19103  
[Wisniewski.patti-kay@epa.gov](mailto:Wisniewski.patti-kay@epa.gov)

Dated: February 8, 2023



\_\_\_\_\_  
Darsh Singh  
FirstEnergy Service Company  
2800 Pottsville Pike  
P.O. Box 16001  
Reading, PA 19612-6001  
(610) 212-8331  
[singhd@firstenergycorp.com](mailto:singhd@firstenergycorp.com)