PENNSYLVANIA
PUBLIC UTILITY COMMISSION
Harrisburg, PA 17105-3265

Public Meeting held June 18, 2026

Commissioners Present:

Stephen M. DeFrank, Chairman
Kimberly Barrow, Vice Chair
Kathryn L. Zerfuss
John F. Coleman, Jr.
Ralph V. Yanora

Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting

Docket No. L-2022-3034353

NOTICE OF PROPOSED RULEMAKING ORDER

BY THE COMMISSION:

In this Notice of Proposed Rulemaking (NOPR), the Pennsylvania Public Utility Commission (PUC) proposes regulations requiring jurisdictional public utilities to report covered cybersecurity incidents and conform to specific standards and frameworks, namely the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), as well as maintain and adhere to specific evaluations, programs, and plans based on the number of customers each public utility serves. The proposed regulations would also mandate each public utility to file annually with the PUC a certification that the public utility is in compliance with the specified standards and requirements. The PUC's proposal provides for a public utility to file a petition for waiver of the cybersecurity evaluation, plan, or program standards if the utility is able to demonstrate that it will maintain and comply with standards that provide a reasonable level of cybersecurity fitness. In this NOPR, the PUC specifically seeks comment about whether electric generation suppliers (EGSs) and natural gas suppliers (EGS) should also be required to maintain and adhere to evaluations, programs, and plans as well as annual

certification with the PUC; these entities are excluded from the definition of public utility in Chapter 102 of the Public Utility Code (Code), 66 Pa.C.S. § 102 (relating to definitions), but are required to be licensed by the PUC.

Second, this NOPR proposed to consolidate cybersecurity incident reporting requirements into a singular chapter of its regulations. The PUC provides in its proposed regulations the incidents that would necessitate a public utility to report to the PUC and a timeline for such reporting. The cybersecurity incident reporting regulation proposes to exclude telecommunications public utilities, consistent with the PUC's prior decisions relating to Chapter 30 of the Public Utility Code, 66 Pa.C.S. Ch. 30, while continuing to require telecommunications utilities to comply with 52 Pa. Code § 67.1 (relating to service outages). The PUC specifically invites comment on whether telecommunications public utilities should remain exempt from the proposed cybersecurity incident reporting requirements.

I. Background

On September 23, 2011, the PUC entered a 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, Docket No. L-2009-2104274 (*2011 Rulemaking Order*), wherein it expanded its regulations to capture more reportable events, in particular cybersecurity attacks, and established deadlines for reporting such accidents. *2011 Rulemaking Order Annex A*.

Subsequently, on August 3, 2017, the PUC entered a Final Rulemaking Order, Final Rulemaking Re Steam Heat Distribution System Safety Regulations, 52 Pa. Code Chapters 61 and 67, Docket No. L-2015-2498111 (*2017 Rulemaking Order* at 22), which extended similar accident reporting requirements to jurisdictional steam distribution utilities. *2017 Rulemaking Order Annex A*. The *2017 Rulemaking Order* also required

steam utilities to develop and maintain a cybersecurity plan, as codified in 52 Pa. Code § 61.45(a), consistent with Chapter 101 of the PUC's regulations. *2017 Rulemaking Order* at 13.

A. ANOPR

At its November 10, 2022, Public Meeting, the PUC adopted an Advance Notice of Proposed Rulemaking at Docket No. L-2022-3034353 (ANOPR) to review its current regulations relating to cybersecurity.[1] These regulations fall into two groups: (1) cyber attack reporting regulations;[2] and (2) self-certification regulations[3] (collectively, existing regulations).

In the ANOPR, the Commission sought comments from interested stakeholders, including members of the regulated industry, statutory advocates, the public, and any other interested parties about whether the existing regulations were sufficient or if they needed to be revised in the face of current and anticipated future cybersecurity threat landscapes.[4] The ANOPR requested that comments be organized around several topics, including:

- Updating Terms and Concepts,
- Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities,
- Improving the Self-Certification Form (SCF) Process,
- Updating Cyber Attack Reporting Regulations,
- Merging the Self-Certification and Cyber Attack Reporting Regulations,
- Cost-Benefit Analysis,
- Eliminating Regulatory Duplication and Overlap,
- Other Matters.[5]

---

[1] *Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Advance Notice of Proposed Rulemaking*, Pa. PUC Docket No. L-2022-3034353, at 1 (Nov. 10, 2022) (ANOPR).

[2] Cyber attack reporting regulations include: 52 Pa. Code §§ 57.11 for electricity public utilities, 59.11 for gas public utilities, 61.11 for steam utilities, and 65.2 for water public utilities.

[3] Self-certification regulations include: 52 Pa. Code §§ 101.1-101.7 for jurisdictional utilities, and § 61.45 for steam utilities.

[4] ANOPR at 2.

[5] *Id.* at 8-21, Appendix A (re: Topics for Comment) provided fifteen specific questions for commenters' consideration.

Nineteen comments were timely filed in response to the ANOPR by AT&T Corp., Teleport Communications America, LLC and SBC Long Distance, LLC (AT&T), the Broadband Communications Association of Pennsylvania (BCAP), Citizens' Electric Company of Lewisburg, Pa., Wellsboro Electric Company and Valley Energy, Inc. (C&T Utilities), Columbia Gas of Pennsylvania, Inc. (Columbia Gas), Duquesne Light Company (Duquesne), Energy Association of Pennsylvania (EAP), FirstEnergy Pennsylvania Electric Company (FirstEnergy), NRG Energy, Inc. (NRG), Office of Consumer Advocate (OCA), Pennsylvania-American Water Company (PAWC), Pennsylvania Chamber of Business and Industry (PA Chamber), PECO Energy Company (PECO), Pennsylvania Telephone Association (PTA), PPL Electric Utilities Corporation (PPL), Retail Energy Supply Association (RESA), United States Environmental Protection Agency Region III (EPA Region III), and Verizon Pennsylvania LLC, Verizon North LLC, MCImetro Access Transmission Services LLC, MCI Communications Services LLC, XO Communications Services, LLC, Verizon Long Distance LLC, and Verizon Select Services Inc. (collectively, Verizon).

The following entities submitted Joint Comments: Aqua Pennsylvania, Inc. and Peoples Natural Gas Company LLC (Aqua/Peoples), Community Utilities of Pennsylvania Inc. and Columbia Water Company (CUPA/CWC), and Tri-Co Connections, LLC and Claverack Communications, LLC (TCC/CC).

B. Supplemental ANOPR

Subsequently, at its April 24, 2025 Public Meeting, the Commission adopted a Supplemental ANOPR at Docket No. L-2022-3034353 to continue reviewing its current regulations relating to cybersecurity.[6] In the Supplemental ANOPR, the PUC discussed

[6] *Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Supplemental Advance Notice of Proposed Rulemaking*, Docket No. L-2022-3034353, at 2 (Apr. 24, 2025) (Supplemental ANOPR).

multiple recent cybersecurity standards updates,[7] noted several significant events in cyber security,[8] and addressed, generally, the following specific topics:

- Ongoing Threats to Critical Infrastructure,
- Moving Towards Defined Cybersecurity Standards,
- Harmonizing PUC Incident Reporting Regulations with the Cybersecurity and Infrastructure Security Agency's (CISA) rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),
- PUC Staff Working Proposals.

The PUC organized thirteen additional questions for stakeholder comments around the following issues:

- Cybersecurity Fitness Standards,
- Cyber Incident Reporting,
- Eliminating Regulatory Duplication and Overlap,
- Other General Considerations

A total of fourteen comments were timely filed in response to the Supplemental ANOPR by AT&T, Aqua/Peoples, BCAP, C&T Utilities, Columbia Gas, Duquesne, EAP, FirstEnergy, National Fuel Gas Distribution Corporation (NFG), PAWC, PB Transport LLC (PB Transport), PECO, PPL, PTA, and Verizon.

Upon consideration of the entirety of the stakeholder comments received by the PUC in response to the initial ANOPR and Supplemental ANOPR, we hereby enter this Notice of Proposed Rulemaking Order (NOPR) setting forth proposed amendments to sections 57.11 (relating to accident reporting for electricity public utilities); 59.11

[7] These updates included: (1) the March 2023 National Cybersecurity Strategy released by the Biden Administration, (2) the February 2024 National Association of Regulatory Utility Commissioners (NARUC) Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources, (3) the March 2024 White House Letter to Governors on Water & Wastewater Systems, (4) the April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience, and (5) the June 2024 Department of Homeland Security (DHS) Memorandum on Strategic Guidance for U.S. Critical Infrastructure. Supplemental ANOPR at 6-9.

[8] The discussed events included the Iranian Islamic Revolutionary Guard Corps (IRGC) accessing multiple US-based water and wastewater systems beginning in November 2023, which included the Municipal Water Authority of Aliquippa; and hackers sponsored by the People's Republic of China (PRC) infiltrating U.S. telecommunications companies in the "Salt Typhoon." Supplemental ANOPR at 11-12.

(relating to accident reporting for gas public utilities); 61.11 (relating to accident reporting for steam utilities); 61.45 (relating to security planning and emergency contact lists for steam heating service); and 65.2 (relating to accident reporting for water public utilities); Chapter 101 (relating to public utility preparedness through self certification); as well as adding new chapters 103 (relating to cybersecurity evaluations, programs, standards, and plans) and 104 (relating to cybersecurity incident reporting), as described below and incorporated within Annex A.

II. Statutory Authority For The PUC's New Or Revised Cybersecurity Regulations

Though previously discussed in our ANOPR, the statutory bases for both the cyber attack reporting regulations and the self-certification regulations are Sections 501, 504, 505, 506, and 1501 of the Public Utility Code (Code), 66 Pa.C.S. §§ 501, 504, 505, 506 and 1501.[9]

Section 501 (relating to general powers) grants the PUC the "general administrative power and authority to supervise and regulate all public utilities doing business within this Commonwealth" and to "make such regulations, not inconsistent with law, as may be necessary or proper in the exercise of its powers or for the performance of its duties."

Section 504 (relating to reports by public utilities), in pertinent part, authorizes the PUC to:

> [R]equire any public utility to file periodical reports, at such times, and in such form, and of such content, as the commission may prescribe, and special reports concerning any matter whatsoever about which the commission is authorized to inquire, or to keep itself informed, or which it is required to enforce . . .[and to] . . .require any public utility to

[9] Chapter 101 Order at 29; Outage Response Order at 36.

> file with it a copy of any report filed by such public utility with any Federal department or regulatory body.

Section 505 (relating to duty to furnish information to commission; cooperation in valuing property) requires that:

> Every public utility shall furnish to the commission, from time to time, and as the commission may require, all accounts, inventories, appraisals, valuations, maps, profiles, reports of engineers, books, papers, records, and other documents or memoranda, or copies of any and all of them, in aid of any inspection, examination, inquiry, investigation, or hearing, or in aid of any determination of the value of its property, or any portion thereof, and shall cooperate with the commission in the work of the valuation of its property, or any portion thereof, and shall furnish any and all other information to the commission, as the commission may require, in any inspection, examination, inquiry, investigation, hearing, or determination of such value of its property, or any portion thereof.

Section 506 (relating to inspection of facilities and records), in pertinent part, empowers the PUC:

> [T]o enter upon the premises, buildings, machinery, system, plant, and equipment, and make any inspection, valuation, physical examination, inquiry, or investigation of any and all plant and equipment, facilities, property, and pertinent records, books, papers, accounts, maps, inventories, appraisals, valuations, memoranda, documents, or effects whatsoever, of any public utility, or prepared or kept for it by others, and to hold any hearing for such purposes [. . . and . . .] have access to, and use any books, records, or documents in the possession of, any department, board, or commission of the Commonwealth, or any political subdivision thereof.

Section 1501 (relating to character of service and facilities), in pertinent part, provides that:

> Every public utility shall furnish and maintain adequate, efficient, safe, and reasonable service and facilities, and shall make all such repairs, changes, alterations, substitutions,

> extensions, and improvements in or to such service and facilities as shall be necessary or proper for the accommodation, convenience, and safety of its patrons, employees, and the public.

The cyber attack reporting regulations also relied on 66 Pa.C.S. § 3009(b) and (d).[10] However, Section 3009 was repealed by Section 1 of the act of November 30, 2004 (P.L. 1398) and replaced by 66 Pa.C.S. § 3019 (relating to additional powers and duties).

The PUC is of the opinion that these statutory provisions of the Code cited above grant it authority to require public utilities to comply with the standards defined in proposed Chapter 103 and with cyber incident reporting requirements as described in proposed Chapter 104.

III. The Cybersecurity And Infrastructure Security Agency's Implementation Of Cyber Incident Reporting For Critical Infrastructure Act Of 2022

In 2022, Congress enacted the Federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[11] which provided for critical infrastructure operators to report covered cybersecurity incidents to the Federal Cybersecurity and Infrastructure Security Agency (CISA). In our ANOPR, the PUC noted that depending on the outcome of its cybersecurity rulemaking proceeding, CISA could designate any or all critical infrastructure sectors, including communications, energy and water and wastewater systems sectors, as covered by CIRCIA's reporting requirements.[12] As such, several stakeholders provided comments on the impact of the CIRCIA on the PUC's efforts to initiate this cybersecurity rulemaking.

[10] Outage Response Order at 36.
[11] Consolidated Appropriations Act of 2022 (Pub. L. No. 117-103) (Mar. 15, 2022). Division Y of this act is the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (6 U.S.C. §§ 681, *et seq*.)
[12] ANOPR at 20.

A. Comments To The PUC's ANOPR Related To CISA's Implementation Of CIRCIA And The Sufficiency Of The PUC's Existing CybersecurityRegulations

In Comments to our ANOPR, AT&T recommended that the PUC assess the information sharing resources and tools to be rolled out by CISA pursuant to its ongoing rulemaking to implement CIRCIA as well as existing public-private partnerships.[13] Likewise, Verizon suggested that the PUC postpone any official rulemaking to update its cybersecurity self-certification regulations until after CISA publishes its final regulations implementing CIRCIA.[14] At that point, Verizon averred that the "PUC will be in a better position to determine what, if any, state cybersecurity self-certification regulations are still necessary in consideration of the costs and benefits of state-specific requirements and the avoidance of duplication with federal rules."[15] Verizon opined that now is not the time for the PUC to open a rulemaking to change its regulations in this area because significant proceedings are ongoing at the federal level, the results of which will inform the PUC's review of its own rules.[16]

Similarly, BCAP recommended that the PUC should delay adoption of any new or revised cyber attack reporting rules until the pending proceeding by CISA to implement CIRCIA is complete, and that new or revised cybersecurity certification or planning rules in Pennsylvania should reflect the success of voluntary, public-private partnership efforts such as the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST).[17]

C&T Utilities stated that each company undertakes company-specific efforts based on its unique network and equipment configurations, that cybersecurity plans are

[13] AT&T Comments at 2.
[14] *Id*. at 8.
[15] *Id*.
[16] *Id*.
[17] BCAP Comments at 2.

evaluated periodically to ensure that current threats are adequately and proactively addressed, and that the C&T Utilities' networks undergo regular scanning and testing under the plans.[18] EAP and Columbia Gas averred that the PUC's existing regulations requiring self-certification and the specific cyber incident reporting criteria are appropriate and remain relevant and consistent with what other states require.[19] CUPA/CWC urged the PUC to exercise caution if it creates new cybersecurity standards that apply to jurisdictional public utilities, and to appropriately balance safety, security, cost, and flexibility.[20]

FirstEnergy posited that the PUC's existing cybersecurity regulations do not need to be revised.[21] However, to the extent the PUC does revise existing regulations, FirstEnergy recommended a "result-based" approach, which 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. [22] PTA stated that the PUC's current self-certification framework is adequate, especially in light of current federal requirements, pending federal legislation, and the recent release of a concept paper from NIST, which will help guide companies and federal agencies on changes in cybersecurity.[23] TCC/CC urged the PUC to conclude that changes are not needed regarding self-certification and cyber attack reporting requirements for jurisdictional telecommunications entities.[24]

PECO recommended that the PUC consider the significant progress that utilities have made to align their programs with industry standards and other federal

[18] C&T Utilities Comments at 1-2.
[19] *Id*. *See also*, Columbia Gas Comments at 2, CUPA/CWC Comments at 3.
[20] CUPA/CWC Comments at 2.
[21] FirstEnergy Comments at 2.
[22] *Id.*
[23] PTA Comments at 1.
[24] TCC/CC Comments at 2.

requirements, including the NIST CSF, that incorporate strong cybersecurity controls and best practices.[25]

PAWC noted that due to the passage of time since the PUC's initial cybersecurity regulations were adopted, as well as recent federal legislation changes related to cybersecurity, limited changes to the PUC's regulations are needed.[26] PPL stated that its cybersecurity strategy are aligned with and informed by, *inter alia*, the NIST CSF and the NERC Critical Infrastructure Protection (CIP) mandatory standards.[27] PPL continued that certain utilities are currently subject to the cybersecurity reporting requirements of NERC, the Federal Energy Regulatory Commission (FERC), the Transportation Security Administration (TSA), the U.S. Department of Energy (DOE), and other federal agencies.[28] PPL averred that the PUC should take those existing requirements into account before laying on additional, redundant, or even perhaps conflicting requirements.[29] Similar to PPL, Aqua/Peoples recommended that any revised regulations be consistent with federal requirements, non-duplicative, and not require a specific framework given the scope of regulated utilities a potential rulemaking will impact.[30]

The PA Chamber opined that, generally speaking, the "PUC's existing regulations rightly recognize there is no 'one-size-fits-all' approach that is appropriate to require of every regulated utility.[31] The PA Chamber posited that the non-prescriptive nature of these regulations, notably the use of a self-certification, is logical and appropriate, especially given the requirements already imposed on utilities by financial institutions

[25] PECO Comments at 2.
[26] PAWC Comments at 2.
[27] PPL Comments at 2.
[28] *Id*. at 3.
[29] *Id*.
[30] Aqua/Peoples Comments at 3.
[31] PA Chamber Comments at 1.

and insurers to ensure operational continuity and mitigation of financial losses due to a data breach or disruption.[32]

Meanwhile, the OCA critiqued the current regulations' reliance on self-certification because they permit the PUC to review utility cybersecurity plans and programs, but only upon request.[33] OCA further averred that it is important for the PUC's regulations to focus on the impact to Pennsylvania retail customers when a utility's cyber-based technologies and systems are attacked or breached and noted that public utilities often house smart meter data with a third-party contractor.[34] The OCA decried the lack of any discussion of the risks associated with reliance by the utility on third party agents for crucial functions that expose customer information to potential unauthorized use or exposure.[35] The OCA also criticized the current regulations on the basis that they "fail to address the need for more public awareness of cybersecurity and each utility's cyber programs and plans."[36]

B. Supplemental ANOPR Related To CISA's Implementation Of CIRCIA

The PUC agreed with commenters to its ANOPR that the CISA rulemaking to implement CIRCIA will reveal important insights and that the Commission should strive to align its reporting requirements, as appropriate, with CISA. However, we also noted two potential limitations to alignment. First, CIRCIA does not provide, nor propose, that incident reports be shared with state agencies like the PUC. Thus, the fact that public utilities will be required to submit CIRCIA incident reports to CISA would have no practical benefit to the PUC or assist with its mission to ensure adequate, safe and reliable

[32] *Id*.
[33] OCA Comments at 2.
[34] *Id*.
[35] *Id*.
[36] *Id*.

public utility service in Pennsylvania.[37] Second, CISA's goals in collecting incident reports are markedly different from the PUC's goals. CISA intends to collect a large volume of incident reports to enable it to participate in real-time trend analysis, information sharing and responding to specific attacks.[38] By contrast, the PUC's incident reporting regulations are limited to keeping the PUC 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.[39] Consequently, the PUC decided to seek additional information on the impact of CSIA's implementation of CIRCIA by issuing a Supplemental ANOPR.

C. Comments To The Supplemental ANOPR Related To The Interplay Between The PUC's Proposal To Amend Its Cybersecurity Regulations And The Implementation Of CIRCIA

As stated above, in its Supplemental ANOPR, the PUC sought comment from stakeholders on whether and how CIRCIA and/or CISA's implementation of CIRCIA creates a potential for regulatory duplication or overlap, given that nothing in CIRCIA or CISA's NOPR to implement CIRCIA contemplates CISA sharing any cyber incident information with the Commission.[40]

AT&T stated that the PUC should not duplicate the functions of Information Sharing and Analysis Centers (ISACs) but could redistribute the information that ISACs

[37] *See* 66 Pa.C.S. § 1501.
[38] CISA NPRM at 23652 ("If CISA designs the proposed regulations in a way that overly limits the quantity and variety of reports it receives from across critical infrastructure sectors, CISA will lack sufficient information to support reliable trend analysis, vulnerability identification, provision of early warnings, and other key purposes of the proposed regulation as indicated by CIRCIA.").
[39] *See*, Joint Statement of Chairperson Robert F. Powelson and Vice Chairperson John F. Coleman, Pa. PUC Docket No. L-2009-2104274, Utilities' Service Outage Response and Restoration Practices, Pa.B. Vol. 42, Number 1, at 9, 20 (Jan. 7, 2012) (emphasizing role of Commission accident reporting regulations in ensuring coordination between Commission, regulated utilities, the Pennsylvania Emergency Management Agency (PEMA) and cities and municipalities in the event of incidents involving widespread utility service outages).
[40] Supplemental ANOPR, Appendix A.

provide via alerts; but any "hands-on threat assessments and responses should remain with the utilities and federal agencies charged with that responsibility."[41] Verizon and BCAP restated its position that the PUC should continue to await the completion of the ongoing CISA rulemaking to craft federal rules implementing CIRCIA for cyber incident reporting and related issues prior to taking action on its own.[42] Verizon further advocated that the PUC rely on the extensive multi-agency federal cybersecurity framework to avoid duplicative state requirements.[43]

FirstEnergy found the CISA NOPR to implement CIRCIA to have significant issues; insofar as duplication exists in form, FirstEnergy recommended that the PUC accept reports in various formats including any mandated by CIRCIA.[44] FirstEnergy posited that otherwise, to be effective, such cybersecurity reporting to the PUC must require the correct amount of specificity to avoid unrealistic and burdensome reporting requirements that will not ultimately provide regulators with the relevant information necessary to stay appraised of malicious breaches to the system.[45] Duquesne noted that although CIRCIA and CISA's proposed rules do not require sharing cyber incident data with state public utility commissions like the PUC, their implementation could still lead to regulatory overlap through parallel reporting obligations and differing definitions of reportable incidents, resulting in confusion, increased administrative burdens on utilities, and fragmented oversight.[46] To avoid duplication and enhance coordination, Duquesne recommended that the PUC align its reporting requirements with federal standards and explore data-sharing agreements with CISA.[47] PPL stated that they cannot definitively determine whether there would be overlap with CISA's implementation of CIRCIA at

[41] AT&T Comments at 15.
[42] Verizon Comments at 1, BCAP Comments at 2, 12.
[43] *Id.* at 1-2, 19.
[44] FirstEnergy Comments at 9.
[45] *Id.* at 10.
[46] Duquesne Comments at 12.
[47] *Id.*

this time, but recommended that the PUC collaborate with other agencies, such as CISA, to avoid any potential overlapping regulatory requirements.[48]

PECO noted that once CIRCIA's final rule is in effect, public utilities will likely be required to report substantial cyber incidents to CISA, and that many of those reportable incidents to CISA would likely trigger reporting obligations to the PUC under the Supplemental ANOPR's Appendix B (regarding Staff Working Proposals); PECO averred that without coordination, this will result in the reporting of different information, with differing timing requirements, to two different entities all for the same event. PECO continued that, were the PUC to adopt CIRCIA's reporting framework, the failure of CISA to share its report information with the PUC would merely result in the duplication of transmission and public utilities could submit to the PUC what they are submitting to CIRCIA with minimal burden.[49]

Aqua/Peoples noted that if the PUC imposes parallel reporting obligations without harmonization with the federal procedures, public utilities may face duplicative compliance burdens that divert resources from actual incident response.[50] EAP noted that there already exists an extensive federal regulatory framework under which many Pennsylvania public utilities are already subject to rigorous federal cybersecurity regulation; these regulatory frameworks include FERC/NERC CIP Standards, TSA Pipeline Security Directives, and CISA/CIRCIA Requirements.[51] EAP recommended that rather than seek to institute new reporting requirements, the PUC should avoid duplicating federal mandates and instead focus on facilitating coordination with federal agencies and monitoring high-level compliance indicators, not prescriptive controls.[52]

[48] PPL Comments at 9.
[49] PECO Comments at 20-21.
[50] Aqua/Peoples Comments at 6.
[51] EAP Comments at 8.
[52] *Id.*

Columbia recommended that minimal changes to the PUC's rules should be considered because the existing regulations are appropriate to meet the PUC's goals without unnecessary duplication with federal government and other agencies' requirements; Columbia anticipates the potential for regulatory duplication and/or overlap in the reporting context.[53]

D. Comments To The Supplemental ANOPR Related To How The PUC Might Eliminate Duplication Or Overlap With CIRCIA

The PUC also asked in its Supplemental ANOPR how it should eliminate regulatory duplication or overlap.[54] Verizon offered that the Commission could avoid regulatory duplication or overlap by permitting companies to certify their compliance with federal rules without additional state requirements.[55] FirstEnergy advocated that state utility commissions hold jurisdictional utilities reasonably accountable for cybersecurity without creating undue burden, and suggested that the Commission not substantially deviate from other states or the guidance of the National Association of Regulatory Utility Commissions (NARUC), as doing so would translate to added costs for the purpose of completing and filing compliance paperwork.[56]

Duquesne recommended that to eliminate regulatory duplication, the PUC should clearly articulate the criteria for determining what assets are in-scope for new requirements, advising that any state requirements should clearly exclude assets already under FERC jurisdiction, per the NERC CIP Reliability Standards. Duquesne further averred that of those assets not covered by federal requirements, the PUC should create clear criteria to avoid applying unnecessary and excessive requirements to minimal risk assets.[57] PPL stated that collaboration among agencies can help the PUC eliminate

[53] Columbia Comments at 2, 9.
[54] Supplemental ANOPR, Appendix A.
[55] Verizon Comments at 19.
[56] FirstEnergy Comments at 10-11.
[57] Duquesne Comments at 13.

regulatory duplication or overlap and recommended that, to the extent that agency collaboration is not feasible, the PUC consider implementing or adopting existing cybersecurity standards and frameworks already applicable to jurisdictional public utilities, including reporting requirements, to prevent regulatory overlap.[58]

PECO averred that the PUC can eliminate regulatory duplication/overlap by accepting compliance with federal cybersecurity regulations for assets subject to applicable requirements and by allowing alignment of remaining assets used to provide service in Pennsylvania with NIST CSF. PECO recommended that the PUC allow utilities to demonstrate compliance through periodic self-certification and maintain sensitive compliance documents onsite subject to review.[59] PECO further suggested that the PUC align with existing federal reporting requirements, formats, and timelines, ensuring efficiency while maintaining the PUC's statutory role by requesting a copy of any federally submitted incident reports rather than imposing a separate incident reporting regime.[60]

PAWC stated that the PUC could eliminate regulatory duplication by allowing a public utility to submit certification that its cybersecurity programs and plans use equal or stricter standards and frameworks than the PUC's regulations require.[61] Aqua/Peoples recommended that the PUC align with federal standards and leverage existing reporting mechanisms in order to enhance cybersecurity oversight while minimizing unnecessary regulatory friction and overlap.[62]

EAP stated that the PUC should avoid duplicating federal mandates and instead focus on facilitating coordination with federal agencies and monitoring high-level

[58] PPL Comments at 9.
[59] PECO Comments at 21.
[60] *Id.*
[61] PAWC Comments at 4, 10.
[62] Aqua/Peoples Comments at 6.

compliance indicators, not prescriptive controls.[63] Columbia advocated for the PUC to mandate adoption of existing, widely recognized, cybersecurity programs rather than developing separate or duplicate standards.[64] PB Transport recommended that the PUC prioritize harmonizing its self-certification requirements and cybersecurity reporting with federal frameworks; it specifically recommended that the PUC adopt CIRCIA's definition of a "cyber incident," as well as its 72-hour reporting timeline, to reduce duplication of reporting burdens and to ensure consistency across jurisdictions.[65]

E. Disposition

While the PUC recognizes that CISA's forthcoming rules implementing CIRCIA may impose duplicative reporting obligations, we are also aware of the delays in such rules being adopted and, as identified above, the fact that CISA's rulemaking may not align with the aims of the PUC in the instant NOPR proceeding. Originally, CISA intended to publish its final rule implementing CIRCIA in October 2025. From there, it was expected that CISA would hold implementation until sometime in 2026 to allow time for potential Congress Review Act procedures.[66] In September of 2025, CISA announced that the publication of its final role had been postponed until May 2026.[67] In March of 2026, it was then announced that due to the ongoing federal government lockdown, the town hall meetings to discuss the rule that were originally planned between March 9 and April 2, 2026, had been postponed. Due to this, CISA announced that the final rule implementing CIRCIA would "likely result in a delay," though CISA did not announce a new expected date.[68] Against this regulatory backdrop, the PUC has

[63] EAP Comments at 8.
[64] Columbia Comments at 9-10.
[65] PB Transport Comments at 1.
[66] https://www.congress.gov/crs-product/R48025, at n. 3. (Last accessed May 26, 2026)
[67] https://industrialcyber.co/cisa/cisa-moves-to-finalize-circia-rules-by-2026-eyes-streamlined-cyber-reporting/, (Last accessed May 26, 2026)
[68] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia, (Last accessed May 26, 2026)

decided to proceed with its NOPR proceeding despite the potential for duplication or overlap between CISA and the PUC.

Still, the PUC's proposed regulations allow for the acceptance of cybersecurity incident reports that utilities submit to federal agencies, where those reports are sufficient for the Commission's purposes. Also, the PUC's proposed regulations permit jurisdictional public utilities to seek waivers of cybersecurity requirements based on meeting specific criteria. This will permit public utilities to avoid unnecessary costs associated with achieving compliance with multiple, overlapping cybersecurity regulatory regimes, while providing the Commission with assurance that adequate measures are in place.

Thus, in light of the stakeholder comments that were submitted in response to the ANOPR and addressed the impact of the enactment of CIRCIA on the PUC's cybersecurity proposals and the comments directly below, as well as the ongoing delays by CISA to implement CIRCIA, the PUC proposes to move forward with updating its cybersecurity regulations despite the countervailing reasons proffered to wait and the possibility of regulatory duplication or overlap.

IV. Proposed Amendments To Sections 57.11, 59.11, 61.11, 61.45, And 65.2 Of Chapter 52 Of The Pennsylvania Code

The *2011 Rulemaking Order* and *2017 Rulemaking Order* addressed service outage reporting requirements in 52 Pa. Code § 67.1, which currently requires all electric, gas, water, steam and telephone utilities to notify the Commission when the lesser of 2,500 or 5% of their total customers have an unscheduled service interruption in a single event for 6 or more projected consecutive hours. 52 Pa. Code § 67.1(b).[69] With these

[69] The PUC is not proposing amendments to Section 67.1, which means that for a telephone utility that elects to file under Section 67.1 requirements, there is no change from what is currently required. *2011 Rulemaking Order* at 6-7.

two orders, the PUC glommed "cyber attack" onto existing reportable accident requirements in different sections of its regulations for public utilities providing electric service, natural gas service, steam heating service, and water service.

At present, the PUC recognizes that, as cybersecurity concerns continue to evolve and must be addressed, it is prudent to capture cybersecurity incident reporting requirements in a standalone chapter of our regulations. As such, with respect to such reporting requirements, the PUC proposes to remove all existing references to "cyber attack" and "attempts against cyber security measures as defined in Chapter 101 (related to public utility preparedness through self certification)" from sections 57.11, 59.11, and 65.2. In place of these substantive removals to sections 57.11, 59.11, 61.11, and 65.2, the PUC proposes a new chapter, Chapter 104 (re Cybersecurity Incident Reporting), to address reporting requirements, which will be discussed in greater detail below in Section VII. Additionally, the PUC proffers several ministerial edits to language in these sections for purposes of clarity. This most often means placing the word "public" before use of utility or the specific utility type before the same.

Additionally, the PUC proposes to remove the term "cyber attack" and "an attempt to interfere with a steam utility's computers, software and communication networks that support, operate or otherwise interact with the steam utility's operation" from section 61.11. The PUC also proposes to remove the requirement for steam distribution utilities to develop and maintain a plan for cyber security from section 61.45. We propose that cybersecurity evaluation, program, standard, and plan requirements for steam distribution utilities will be located in our newly proposed Chapter 103.

Accordingly, the PUC seeks comment on its proposal to separate into a new chapter cybersecurity incident reporting requirements across public utility sectors from other accident reporting applicable to each distinct public utility sector.

V. Proposed Amendments To Chapter 101 (Relating To Public Utility Preparedness Through Self Certification) And Reserving Sections 101.4 And 101.5

On March 10, 2005, the Commission entered a Revised Final Rulemaking Order, *Rulemaking Re: Public Utility Security Planning and Readiness*, Docket No. L-00040166 (*2005 Rulemaking Order*), that led to the adoption of 52 Pa. Code Ch. 101. At the time, the PUC stated:

> The intent of this rulemaking has always been to improve the security monitoring of our jurisdictional utilities. As mentioned in our prior orders, this rulemaking requires all jurisdictional utilities to develop and maintain written physical security, cyber security, emergency response and business continuity plans to protect the Commonwealth's infrastructure and ensure safe, continuous and reliable utility service. In accordance with the regulations, jurisdictional utilities will submit a Public Utility Security Planning and Readiness Self Certification Form (Self Certification Form) to the Public Utility Commission (Commission) attesting to compliance with [Chapter 101].

2005 Rulemaking Order at 1.

52 Pa. Code § 101.1 (relating to purpose) requires every "jurisdictional utility" to "develop and maintain" a cybersecurity plan "to protect this Commonwealth's infrastructure and ensure safe, continuous and reliable utility service."[70] To ensure compliance, a jurisdictional utility annually submits a Self-Certification Form (SCF) stating that it has a cybersecurity plan in place which the PUC may review upon request.[71] ANOPR at 3. In our ANOPR, the PUC sought 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

[70] Section 101.1 also requires jurisdictional utilities to develop and maintain plans for physical security, emergency response and business continuity.

[71] *See generally* 52 Pa. Code §§ 101.1–101.7 (relating to public utility preparedness through self-certification) (Chapter 101).

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.

Upon review of the comments received to both our ANOPR and Supplemental ANOPR on the topic of the sufficiency of our existing regulations, the PUC proposes to remove the development and maintenance of cybersecurity plans and submission of a SCF from Chapter 101. In order to better accommodate the removal of cybersecurity from Chapter 101, the PUC proposes several non-substantive amendments to Chapter 101 to create greater clarity in its existing regulatory sections relating to physical security, emergency, and business continuity plans.

Additionally, the PUC proposes a new Chapter 103 to address cybersecurity evaluations, programs, standards, and plans more comprehensively. The comments related to the sufficiency of the PUC's existing regulations and the anticipated regulatory language for Chapter 103 will be discussed in greater detail in Section VI.

Accordingly, the PUC seeks comment on its proposal to separate into a new chapter, Chapter 103, cybersecurity evaluations, programs, standards and plans.

VI. Proposed Chapter 103 Relating To Cybersecurity Evaluations, Programs, Standards, And Plans

As stated in the Supplemental ANOPR, the PUC's current Chapter 101 regulations were promulgated in its *2005 Rulemaking Order* and have not been refreshed to reflect state-of-the-art cybersecurity concepts and standards. Thus, there are significant gaps in the cybersecurity standards regimes maintained by federal sector specific agencies. Moreover, federal authorities have increasingly pressed for sector-specific agencies—

including State agencies—to impose objective standards to ensure that critical infrastructure operators are meeting a high level of cybersecurity fitness.[72]

A. ANOPR And Supplemental ANOPR Stakeholder Comments Related To The Sufficiency Of The PUC's Existing Regulations And Imposing Defined Cybersecurity Fitness Standards

Commenters to the ANOPR had mixed views on the prospect of regulating adherence to defined cybersecurity fitness standards. On one hand, PECO opined that, while "the Commission's existing self-certification model is sufficient to address the cybersecurity posture of public utilities in Pennsylvania…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."[73] In that event, PECO cautioned that the Commission should consider whether "the substantial controls already implemented by public utilities like PECO, align with "established cybersecurity frameworks" and "focus on requirements or recommendations that avoid overly prescriptive controls and instead address risk-based objectives that public utilities will have the flexibility to meet through a range of industry-accepted security approaches."[74] On the other hand, the Joint Comments of CUPA and CWC argued that "[c]ompliance with a federal or industry standard is not appropriate given that: (1) different utility sectors are subject to unique risks and requirements; and (2) cybersecurity standards are generally meant to be flexible and are not meant to be applied prescriptively or as a one-size-fits all solution."[75]

In its Supplemental ANOPR, the PUC's first question asked public utilities if the PUC should require jurisdictional utilities to maintain cybersecurity programs and plans

[72] Supplemental ANOPR at 12-13.
[73] Comments of PECO, Pa. PUC Docket No. L-2022-3034353, at 4 (Feb. 8, 2023).
[74] *Id.*
[75] Joint Comments of Community Utilities of Pennsylvania, Inc. and Columbia Water Company, Pa. PUC Docket No. L-2022-3034353, at 2 (Feb. 8, 2023).

that conform to specific standards and frameworks, specifically citing the NIST Cybersecurity Risk Framework, NIST Special Publication 800-53, and NIST Special Publication 800-82.[76] The majority of commenters fell in a middle ground of supporting additional requirements that apply to facilities not already covered by existing standards and frameworks, but also supporting the Commission accepting compliance with existing regulations for those utilities that are already regulated. Both Duquesne and PECO expressed that they would only support additional Commission-imposed requirements when they applied to facilities not already covered.[77] Aqua/Peoples and EAP both recommended allowing utilities to maintain compliance with widely accepted frameworks where such frameworks already exist.[78]

Both FirstEnergy and PPL noted that two of the specific standards listed, NIST Special Publication 800-53 and NIST Special Publication 800-82, would be difficult to conform to.[79] FirstEnergy stated that those standards provided useful guidance, but they did not rise to the level of a complete, assessable standard.[80] PPL stated that requiring conformity to those standards specifically could prove both challenging and costly for public utilities.[81]

Two commenters were firmly against the PUC requiring additional rules and conformity. Verizon stated that if state-specific rules are determined necessary after the completion of CISA's rulemaking, the existing self-certification method should be sufficient without requiring the potential framework detailed by the PUC.[82] PTA averred that requiring conformity with NIST or similar standards is unnecessary and may

[76] Supplemental ANOPR, Appendix A.
[77] Duquesne Supplemental ANOPR Comments at 4; PECO Supplemental ANOPR Comments at 4.
[78] Aqua/Peoples Supplemental ANOPR Comments at 3; EAP Supplemental ANOPR Comments at 3.
[79] FirstEnergy Supplemental ANOPR Comments at 2-3; PPL Supplemental ANOPR Comments at 2.
[80] FirstEnergy Supplemental ANOPR Comments at 3.
[81] PPL Supplemental ANOPR Comments at 2.
[82] Verizon Supplemental ANOPR Comments at 8.

frustrate the Commission's stated objective of avoiding regulatory overlap.[83] C&T Utilities noted that the Commission's use of the word "conform" overlooked the nature of the CSF guidelines, and recommended that alignment with CSF be considered a permissible program design option.[84]

Columbia stated that if the Commission does require utilities to maintain cybersecurity programs, such programs should align with NIST frameworks.[85]

PAWC was the only commenter to state that it believed the Commission should require utilities to maintain cybersecurity programs and plans that conform with specified standards and frameworks without noting specific exceptions.[86]

B. The PUC's Decision To Propose Imposing Defined Cybersecurity Fitness Standards

Notwithstanding the divergent opinions offered in comments to the PUC's ANOPR and Supplemental ANOPR regarding conformity to specific standards and frameworks, the PUC proposes regulations to require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks as set forth in Chapter 103. Given the increasing importance of ensuring that our jurisdictional public utilities are adhering to high standards of cybersecurity fitness, and gaps in federal coverage of at least some of the sectors we regulate, we find regulations requiring adherence to defined standards are advisable. At the same time, we recognize that several of our jurisdictional public utilities have undertaken and maintain cybersecurity programs, plans, and standards that provide a reasonable level of fitness relative to their provision of service in the Commonwealth and that prescriptive regulations in these instances may not be in the public interest. Thus, the PUC provides

[83] PTA Supplemental ANOPR Comments at 2.
[84] C&T Utilities Supplemental ANOPR Comments at 4.
[85] Columbia Supplemental ANOPR Comments at 2.
[86] PAWC Supplemental ANOPR Comments at 2.

an opportunity for a public utility to request waiver in proposed Section 103.5 of the regulation. The PUC seeks informed stakeholder comment on each of the sections, 103.1-103.7 below.

C. 52 Pa. Code Section 103.1. Purpose

Section 103.1 states the intent of the PUC's regulations to ensure that jurisdictional public utilities meet an appropriate level of cybersecurity fitness through the imposition of objective standards as defined by the PUC.

D. 52 Pa. Code Section 103.2. Definitions

In our ANOPR, we sought comment 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.[87]

The C&T Utilities asked the PUC "to remain mindful that certain NERC and other federal cybersecurity requirements may apply only to the larger electric and gas utilities, while smaller utilities are not covered because they do not interact with the bulk electric and gas systems and assert that adopting federal definitions may be too stringent and impose unreasonable requirements on smaller Pennsylvania utilities.[88] CUPA/CWC recommended that, to the extent that new requirements are established, the PUC should ensure that it carefully defines terms so as to be consistent with generally accepted standards, such as the NIST's CSF.[89] Similarly, Duquesne Light agreed that certain terms may need to be updated to reflect current times and practices more fully, and recommends that, to the extent possible, the "PUC use definitions in existing statute or

[87] ANOPR at 9, Appendix A.
[88] C&T Utilities Comments at 5.
[89] CUPA/CWC Comments at 5.

regulation, such as the Pennsylvania Breach of Personal Information Notification Act."[90] EAP suggested that the PUC focus on the information and definitions that are of most interest and actionability by the PUC, items such as interruptions, reliability impacts, or the theft and misuse of Commonwealth residents' information.[91] PAWC advocated for the PUC to remove outdated terminology and promote consistency with federal cybersecurity regulation, including CIRCIA.[92]

1. National Institute Of Standards And Technology And The Computer Security Resource Center

Section 103.2 provides definitions of cybersecurity terms, evaluations, plans, programs, and standards the PUC proposes to use in requiring jurisdictional public utilities to comply with Section 103.3 (relating to cybersecurity evaluations and programs), and that are relevant to Section 103.4 (relating to annual certification). These definitions were primarily drawn from the NIST's Computer Security Resource Center's (CSRC) glossary, which is an aggregation of terms and definitions specified in NIST's cybersecurity and privacy standards, guidelines, and other technical publications.[93] The definitions of these terms may have been modified by the PUC from several offerings or uses to best serve the purposes of our cybersecurity regulations.

2. The Public Utility Code And Title 52

Additionally, the PUC provides definitions for "public utility," "common carrier," "electric utility," "gas utility," "steam utility," "telecommunications utility," "water utility," and "wastewater utility," which reflect Section 102 of the Public Utility Code (Code), 66 Pa.C.S. § 102, or specific provisions of Title 52 of the PUC's regulations where indicated.

---

[90] Duquesne Light Comments at 4.
[91] EAP Comments at 3; *see also* PECO Comments at 6.
[92] PAWC Comments at 2.
[93] The NIST CSRC glossary can be found at https://csrc.nist.gov/glossary (last accessed June 8, 2026.

3. Public Utility Classifications

Next, with regard to definitions, the PUC proposes the creation of five classes of public utilities based primarily on the number of customers a public utility serves, and secondarily on the utility sector and use, or lack thereof, of collecting or storing personal information (PI), use of information technology (IT) and of operational technology (OT). A "class 1 utility" serves 100,000 or more customers, a "class 2 utility" serves at least 3,300 customers but fewer than 100,000 customers, and a "class 3 utility" serves less than 3,300 customers.[94] The definition of a "class 4 utility" addresses common carriers collecting and storing PI, or using IT and OT, specifically. A "class 5 utility" is an electric, gas, steam, water, or wastewater utility that does not collect or store PI, or use IT and OT.

The PUC has determined that "telecommunications utilities" fall outside these five classes due to Section 3015(f) of the Code (re: reports the PUC can require under alternative forms of regulation), 66 Pa.C.S. § 3015(f)(1); *see also*, *Section 3015(f) Review regarding the Lifeline Tracking Report, Accident Report and Service Outage Report,* Docket No. M-00051900, ordering paragraphs 1, 3-4, (entered December 30, 2005).

a. Comments To The Supplemental ANOPR Regarding Classifications

In response to the Supplemental ANOPR, C&T Utilities suggested that aspects of the proposed regulations contained within the Supplemental ANOPR may be overly prescriptive and may intrude on the utility's managerial discretion to design its cybersecurity program; they noted that they are classified as a Class 2 utility in the proposed regulations but aver that the requirements set forth for a Class 1 or 2 utility are

[94] The PUC chose 3,300 customers as a metric because of the Environmental Protection Agency's requirement in Section 1433 of the Safe Water Drinking Act that "each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system. 42 U.S.C.A. § 300i-2.

overly rigid and do not appear to recognize the role of the utility's management and Board of Directors in reviewing and overseeing utility operations.[95] C&T Utilities further averred that the proposed requirements for a Class 3 utility better reflect the appropriate balance for all utilities while ensuring that critical program evaluation occurs and that response programs are in place. C&T Utilities recommended that if the Commission believes that the Class 1 and 2 requirements are needed for some larger utilities, then Class 3 requirements should be adopted for any utility that serves fewer than 100,000 customers and does not possess critical infrastructure or bulk electric system facilities.[96] C&T Utilities recommended specific changes to some of the Class 2 and Class 3 requirements that they view as unnecessarily rigid and not allowing each utility to adopt a program reflecting their individual risks and maturity.[97]

PAWC stated that it may not be appropriate or practical to create new classes solely for the purpose of cybersecurity evaluations, programs, standards and plans (looking at proposed Section 103.1 definitions); PAWC suggested that the tool a utility selects to conduct its cybersecurity evaluation should remain within the discretion of the utility (looking at proposed section 103.2 Cybersecurity Evaluations and Programs).[98] PAWC advocates for the Staff Working Proposals to include a requirement of filing an annual certification that a utility adheres to the cybersecurity evaluations and programs set forth in proposed Section 103.2, but also proposes eliminating the requirement under existing 52 Pa. Code § 101.4 that a utility file a SCF.[99]

[95] C&T Utilities Comments at 10-11.
[96] *Id.* at 11.
[97] *Id.*
[98] PAWC Comments at 11.
[99] *Id.*

b. General Comments To The Supplemental ANOPR Regarding Definitions

With regards to Chapter 103, FirstEnergy believes that aligning certain definitions with other state and federal standards would promote consistency and avoid conflicting interpretations that create uncertainty.[100] FirstEnergy believes the current definition of "asset" is overly broad and does not allow for a risk-based programmatic approach.[101]

FirstEnergy suggested utilizing the term "asset" exclusively throughout Chapter 103, which would remove additional defined terms including: "information technology (IT)," "operational technology (OT)," and "supervisory control and data acquisition (SCADA)."[102] FirstEnergy further suggested replacing the definition of "personal information" (PI) with the statutory reference to "personally identifiable information" (PII) used in the Code, and averred that replacing it with the definition used in the Code would promote clarity and consistency across the board while reducing the risk of conflicting interpretations and ensuring utilities are operating under a common understanding of what constitutes protected information.[103]

FirstEnergy also averred that Chapter 103 presents some workability concerns, offering the example that they suggest the Commission remove the language in Chapter 103 which mandates the use of the "Cybersecurity Evaluation Tool (CSET)" and replace it with more generic language regarding the evaluation of coverage and maturity of a cybersecurity program.[104] FirstEnergy additionally suggested changes to the definition of "security management program" in Chapter 103,[105] and "cyber incident" in Chapter 104.[106]

---

[100] FirstEnergy Comments at 12.
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.* at 13.
[105] *Id.* at 14.
[106] *Id.* at 15.

4. The PUC Invites Comments On Section 103.2 (Relating To Definitions)

The PUC seeks comment on its proposed definitions but specifically solicits comment on its proposal to use the size of a public utility's customer base to determine the cybersecurity evaluations and plans that a utility must develop and maintain. If a commenter advocates that the number of customers a public utility serves is not the correct metric, the PUC requests alternative suggestions be provided.

E. 52 Pa. Code Section 103.3. Cybersecurity Evaluations And Programs

In addition to conformity to specific standards and frameworks as discussed above, in the PUC's Supplemental ANOPR public utilities were queried about whether the PUC should consider the extent and burden of the requirement(s) in relation to the size of the utility.[107]

1. Comments To The Supplemental ANOPR Related To The Size Of A Public Utility's Customer Base As A Metric For Cybersecurity Requirements

Two utilities answered affirmatively that the PUC should consider the burden of requirements in relation to the public utility's size. Verizon suggested that the Commission consider whether and to what extent an industry or utility is already subject to federal requirements, where the Commission could reasonably rely on their self-certification of federal compliance.[108] Columbia recognized that there is a significant financial burden to complying with frameworks like NIST CSF, and advised the Commission to consider implementing alternative recovery mechanisms.[109]

[107] Supplemental ANOPR, Appendix A
[108] Verizon Comments at 9.
[109] Columbia Comments at 3.

A plurality of utilities answered that they did not believe the Commission should consider a utility's size in the requirements. Both PTA and PECO stated that there should not be a need to classify utilities by size or function; PTA averred that continuing the current self-certification process obviated the need for any changes, while PECO argued that adopting an outcome-based approach that leverages NIST CSF should remove the need to classify utilities as such.[110] C&T Utilities recommended that while some assumptions regarding cybersecurity risk could be made based on an organization's size, the risk-based approach should also focus on the types of facilities that the entity manages and the potential harms that may result from a successful cybersecurity threat.[111] Both PAWC and Aqua/Peoples recommended that all public utilities be treated similarly regardless of size or capability, with PAWC favoring the Commission retaining consistency with its existing regulations.[112] Finally, EAP argued in support of the Commission maintaining a flexible, risk-based framework, allowing utilities to continue to tailor their programs to their own operations, risk tolerance, and maturity.[113]

Two utilities offered a middle-ground approach. Duquesne contended that certain baseline requirements should apply to any utility but agreed that it is appropriate to exercise flexibility based on the size and individual characteristics of a utility. As such, Duquesne suggested a tiered approach like the one suggested in the PUC's staff working proposals that were attached to the Supplemental ANOPR, at Appendix A.[114] BCAP stated that the self-certification provisions in the existing rules set forth key plan elements that are integral to ensuring a baseline level of cybersecurity, but agreed that the Commission could provide an alternative means of compliance via self-certification of compliance with a leading federal or industry framework.[115]

[110] PTA Comments at 2; PECO Comments at 8.
[111] C&T Utilities Comments at 5.
[112] PAWC Comments at 2-3; Aqua/Peoples Comments at 4.
[113] EAP Comments at 3-4.
[114] Duquesne Comments at 5.
[115] BCAP Comments at 10.

AT&T, PPL, and PB Transport all stated that the Commission should leverage the existing federal resources and frameworks, with PB Transport noting that the Commission should maintain its current requirement for self-certification but should streamline the process.[116]

2. The PUC's Decision To Use The NIST CSF

In our consideration of options for specific standards and frameworks to apply to jurisdictional public utilities, the PUC reviewed utility sector specific frameworks. For example, the PUC reviewed America's Water Infrastructure Act (AWIA), which amended Section 1433 of the Safe Drinking Water Act, and requires community water systems serving more than 3,300 people to develop or update risk and resilience assessments and emergency response plans. [117] Additionally, the PUC reviewed the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards, which are mandatory for electric utilities and that are audited by ReliabilityFirst, the regional entity for Pennsylvania.[118] With respect to gas utilities operating critical pipeline infrastructure, the PUC evaluated the U.S. Department of Homeland Security's Transportation Security Administration's (DHS-TSA) Security Directive Pipeline-2021-02, which mandates specific security outcomes.[119]

After reviewing the comments provided by stakeholders, the PUC's proposed regulation, at Section 103.3, recommends that public utilities in classes 1-4 be generally required to conform to the NIST CSF. From this NIST CSF baseline, then, each class is subject to additional requirements commensurate with their size (i.e., the number of customers served) and risk profiles. These additional requirements may include written programs aimed at ensuring greater cyber hygiene, and direct specifications for annual

[116] AT&T Comments at 8; PPL Comments at 3; PB Transport Comments at 2.
[117] *See* https://www.epa.gov/waterresilience/awia-section-2013.
[118] *See* https://www.nerc.com/standards/reliability-standards/cip.
[119] *See* tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf.

cybersecurity evaluations.

Separately, for telecommunications utilities, our proposed regulation at 103.3(d) requires the development and maintenance of a written cybersecurity plan and provides minimum specifications for such.

The NIST CSF, which the PUC proposes to use as a foundation in its proposed regulation, is used widely by water, electric and gas utilities. In addition, NIST Special Publication (SP) 800-82 and NIST SP 800-53 have application and overlay across these sectors. Integrating the NIST CSF, SP 800-53, and SP 800-82 into the regulatory framework transforms utility oversight from passive, checklist-based compliance to proactive, continuous risk management. By aligning these foundational standards, the proposed regulations establish a unified technical language that bridges the gap between traditional IT and operational Industrial Control Systems (ICS). This comprehensive mapping ensures that a public utility can consistently assess vulnerabilities, prioritize resources, and deploy targeted security controls. Ultimately, the PUC finds that this structured approach elevates collective defense, enabling public utilities to anticipate, withstand, and rapidly mitigate evolving cyber threats to critical infrastructure.

The PUC seeks comment on its proposal to require conformity to the NIST CSF across utility sectors and on the scope of additional requirements for utilities serving greater numbers of customers.

F. 52 Pa. Code Section 103.4. Annual Certification

Section 103.4 of the PUC's proposed regulation requires each of the first four classes of public utility defined in Section 103.2, as well as telecommunications utilities, to file with the PUC an annual cybersecurity certification that the public utility complies with the corresponding subsection of Section 103.3. Regarding any class 5 utility, an

annual certification is required confirming that the public utility does not collect or store PI, does not use IT, and does not use OT. The PUC, in subsection (f), also proposes the time for each public utility to submit its annual cybersecurity certification.

1. Comments To The Supplemental ANOPR Regarding Self Certification

In response to an enquiry about the use of a SCF in the Supplemental ANOPR, which has been used in Chapter 101 of our current regulations but is being removed from that chapter in order to accommodate the PUC's proposed cybersecurity regulatory scheme, most public utilities recommended that the PUC continue using a self-certification process. AT&T stated that the annual self-certification remains effective, along with Duquesne, who recommended the Commission maintain its current practice of requiring an annual self-certification compliance filing.[120] FirstEnergy recommended that any new self-certification process align directly with the needs and objectives of the Commission to protect the utility services and information of Commonwealth residents, similar to the one currently in place, while also noting that the Commission's existing management audit process serves as a sufficient mechanism for confirming compliance with cybersecurity requirements.[121]

In the same vein, PECO recommended that the Commission continue its current self-certification approach, and specifically recommended that the new rule require jurisdictional utilities to self-certify compliance with federal cybersecurity regulations where applicable, and to align with NIST CSF for their remaining assets that are used to provide public utility service in the Commonwealth.[122] C&T Utilities stated that the current self-certification process is sufficient, and recommended that the Commission's staff's periodic Management Audit review process consider whether particular standards

[120] AT&T Comments at 9; Duquesne Comments at 7.
[121] FirstEnergy Comments at 5-6.
[122] PECO Comments at 10.

or frameworks are reasonable based on the utility's size, type of assets, and personal information collection or storage practices.[123] PAWC stated that they were in favor of annual self-certification, and also believe that an annual certification should be considered confidential.[124] Aqua/Peoples recommended a periodic self-certification process with the ability for Commission staff to review and inspect plans at public utility facilities; they further recommended that certification documents not require disclosure of detailed architecture or system-level data.[125]

Two utilities offered different perspectives. Verizon stated simply that CISA has investigatory and enforcement powers and that the Commission should not duplicate compliance requirements that exist at the federal level.[126] Columbia averred that for jurisdictional utilities, the Commission should accept a Public Utility Security Planning and Readiness SCF, and that for non-utility companies, the Commission should require an entity to certify its cybersecurity fitness.[127]

The PUC looks forward to any additional comments on the requirement of annual certification and the timing to submit the filing annually, as well as on the formatting and filing requirements of such a form.

2. Annual Cybersecurity Certifications Status As Confidential Security Information

In its Supplemental ANOPR, the PUC received comments related to whether each annual cybersecurity certification should be treated as confidential security information (CSI), as defined in 35 P.S. § 2141.2, and how the PUC might accept electronic filings of certifications consistent with the Public Utility Confidential Security Information

[123] C&T Utilities Comments at 5.
[124] PAWC Comments at 5.
[125] Aqua/Peoples Comments at 5.
[126] Verizon Comments at 11.
[127] Columbia Comments at 4-5.

Disclosure Protection Act (CSI Act), 35 P.S. §§ 2141.1-2141.6.

PB Transport recommended that the Commission further clarify how it will safeguard electronic submissions of completed SCFs and ensure that confidential data is not accidentally disclosed.[128]

Three utilities shared middle-of-the-road responses. Verizon averred that any attempt to create a self-certification form that is public and not treated confidentially would need to ensure that it complies with the CSI Act, noting that a "one-size-fits-all" solution may not be appropriate for the self-certification process and that the Commission might need to take a larger role in certifying the cybersecurity fitness of smaller entities or industries.[129] Duquesne stated that an annual certification by a public utility that it adheres to a specific cybersecurity standard could reasonably be considered CSI, depending on the content and context of the certification, further warning that the annual certification, particularly if it discloses non-adherence, could lead to a serious security concern if publicly disclosed.[130] PPL voiced their support for a heightened level of protection of the annual self-certification, particularly if changes are made through this rulemaking process that result in more detailed cybersecurity information being provided to the Commission; they further stated that they did not see a reason to deviate from the Commission's established practices for the treatment and protection of CSI.[131]

The majority of utilities expressed agreement that annual certification be considered CSI. AT&T recommended that along with annual certification being considered CSI, the Commission should implement secure electronic submission portals or secure email gateways.[132] FirstEnergy and Aqua/Peoples both noted that annual

[128] PB Transport Comments at 1.
[129] Verizon Comments at 11-12.
[130] Duquesne Comments at 8-9.
[131] PPL Comments at 5.
[132] AT&T Comments at 10.

certifications being publicly available could allow for targeted attacks by threat actors, suggesting that such disclosures may signal potential weaknesses in cybersecurity posture or compliance readiness; Aqua/Peoples specifically recommended that certification status only be shared with authorized regulatory bodies and not be made publicly accessible.[133] PECO requested that annual certifications be considered CSI regardless of whether they are redacted, and further requested that the Commission carefully consider the deliberations of FERC and NERC on a similar issue in FERC Docket No. AD19-18-000, where both FERC and NERC staff determined that publishing redacted cybersecurity violation and penalty information poses a tangible risk to the electric grid; they also noted that in a similar vein, the public release or unsecure transmission of redacted certifications by Pennsylvania public utilities that indicate alignment with NIST CSF or with federal regulatory requirements would pose a tangible risk to their facilities in the form of their IT and OT systems.[134]

Both C&T Utilities and PAWC simply recommended that the annual certification continue to be considered CSI.[135] EAP recommended a recurring self-certification process with the option for Commission staff to inspect plans and annual certifications at utility facilities, positing that certification documents should not require disclosure of detailed architecture or system-level data.[136] EAP further recommended that annual certifications be treated as CSI, and voiced belief that the PUC's current SCF is consistent with this objective; they also suggested that the Commission adopt an on-site review protocol whereby Commission staff can inspect cybersecurity documents at utility facilities under appropriate confidentiality agreements and security controls.[137] Columbia stated that protections and protocols for Security Sensitive Information (SSI) are similar

[133] FirstEnergy Comments at 6; Aqua/Peoples Comments at 5.
[134] PECO Comments at 13-14.
[135] C&T Utilities Comments at 6; PAWC Comments at 6.
[136] EAP Comments at 4.
[137] *Id.*

to protections for CSI and, thus, should be considered the same.[138]

Based on this general consensus by commenters, as well as the fact that the current SCF referenced in Chapter 101 is treated as CSI and the proposed annual certification is likely to contain similar sensitive information that fits the definition for CSI, the PUC proposes in Section 103.4(g) to treat annual cybersecurity certifications as CSI.

3. Filing Of Annual Cybersecurity Certifications Consistent With The CSI Act

In comments to the PUC's Supplemental ANOPR, AT&T stated that they believe the Commission should implement secure electronic submission using encrypted portals or secure gateways, with limited access.[139] Verizon stated that once the CISA rulemaking is complete, they hope the Commission will determine that certifications or other filings required at the federal level obviate the need for Commission-regulated communications companies to also file at the state level or, at the very least, require simpler, non-confidential certification forms; they further averred that if changes to the handling of this information is found necessary, then such changes should be made in the context of changing that regulation for all public utility CSI.[140] FirstEnergy recommended that the Commission accept reasonable forms of electronic filing, classified as CSI, for disclosure reasons.[141]

Duquesne recommended that the Commission maintain a dedicated, encrypted electronic filing system that: 1) requires multi-factor authentication for access; 2) supports role-based access control with least privilege access control to limit who can view CSI; 3) logs all access and submission activity for audit purposes; 4) enforces labeling and data segregation; 5) enforces encryption at rest and in transit; 6) follows

[138] Columbia Comments at 5.
[139] AT&T Comments at 10.
[140] Verizon Comments at 12-13.
[141] FirstEnergy Comments at 6.

strict protocols for internal sharing and storage of backups; 7) sends a secure acknowledgment receipt to the utility; 8) confirms that the filing has been properly classified and stored; 9) conducts internal audits to ensure internal compliance and transparently share those reports with the utility; and 10) provides guidance documents to utilities on secure filing practices.[142] Duquesne went on to reiterate that a self-certification form similar to that currently filed may be most appropriate to avoid the disclosure of potentially sensitive information, and that in order to limit the Commission's risk of being a target for bad actors seeking to access utility data, the Commission should avoid including highly sensitive information on the annual certification.[143]

PPL stated that they do not see a reason to deviate from the Commission's established practices for the treatment and protection of CSI.[144] PECO suggested that 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; alternatively, PECO proposed 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 is up-to-date.[145] PECO further noted that this approach would be consistent with their 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.[146]

[142] Duquesne Comments at 9.
[143] *Id.*
[144] PPL Comments at 6.
[145] PECO Comments at 14.
[146] *Id.* at 15.

C&T Utilities recommended that the self-certification be a very short confirmation that a cybersecurity plan is maintained and available at the utility's offices.[147] PAWC suggested that the Commission look at other jurisdictions to methods to accept electronic filings consistent with CSI Act.[148] Aqua/Peoples recommended that the Commission enact an on-site review standard whereby Commission staff can review cybersecurity documents at the utility's secure location under confidentiality agreements, noting that these in-person reviews provide the Commission with access to utility cybersecurity preparedness without creating additional attack vulnerabilities, and that it is consistent with established practices in other regulated industries where sensitive security information requires direct oversight.[149] Columbia recommended that the Commission collaborate with CISA or other federal agencies to determine best practices and implement a solution that is validated by an independent assessment to ensure the Commission can securely store information.[150]

The PUC's proposed rulemaking at Section 103.4(f) recommends the creation of a secure portal to allow public utilities to streamline the filing of annual cybersecurity certification. The PUC seeks additional comment on this proposal.

4. Considering Annual Certification Requirements For Electric Generation Suppliers (EGSs) And Natural Gas Suppliers (NGSs)

As presently drafted, the PUC's cybersecurity regulations do not require EGSs or NGSs to submit annual certifications to the PUC as is mandatory for jurisdictional public utilities. These entities are not public utilities pursuant to the Code; however, they are required to be licensed in Sections 2208 (re: requirements for natural gas suppliers) and 2809 (re: requirements for electric generation suppliers.

[147] C&T Utilities Comments at 6.
[148] PAWC Comments at 6.
[149] Aqua/Peoples Comments at 5-6.
[150] Columbia Comments at 5-6.

In our ANOPR, the PUC sought comment on whether the self-certification requirements in our existing regulations should be extended to apply to additional entities subject to the PUC's supervision, like EGSs and NGSs. A range of opinions were provided in response.

Duquesne suggested that those entities with access to customer information be required to ensure such information is kept confidential and prove themselves fit technically to ensure cybersecurity is maintained. Duquesne posited that it may be appropriate to require electric generation suppliers (EGSs) to submit the SCF as they have access to customer data and sensitive information through electronic data interchange (EDI) and other avenues.[151] FirstEnergy stated that the entities with whom its subsidiaries exchange sensitive data are often not required to certify any type of cyber fitness by the PUC, and suggests that the PUC "consider self-certification requirements for the various entities that are players in today's market."[152]

The OCA recommends the PUC to require licensed energy suppliers (electric and gas) who gather and make use of private customer data be included in the forthcoming regulations, noting that these entities gather customer information for the purposes of enrollment, billing, complaint handling, and customer service.[153] OCA recommended the PUC to "inquire of these entities of their cybersecurity plans and programs at the time of licensure or renewal of license, including the location of where the customer data will be housed, what existing cybersecurity regulations are applicable to that data at the location where it is housed, and oblige these entities to inform the PUC of any breach in their customer data and what steps were taken to notify affected customers and what remedial action was taken in response." OCA further recommends that repeated instances of misuse or breach of customer data should be grounds for license revocation.[154]

[151] Duquesne Light Comments at 7.
[152] FirstEnergy Comments at 14-15.
[153] OCA Comments at 5.
[154] *Id*.

NRG and RESA stated that NGSs and EGSs are expressly excluded from the definition of "public utility" in the Code except for limited purposes and, therefore, the PUC's regulations under consideration here do not impose cyber attack reporting or self-certification filings on the NGSs or EGSs.[155]

RESA suggested that the PUC first consider whether the level of interaction between the systems of NGS/EGS and utility systems is sufficient to warrant extending reporting requirements to the NGS/EGS.[156] If the PUC finds that such an extension is needed, RESA urged the PUC to not apply a one-size-fits-all approach and to recognize that certain entities, such as suppliers, pose a substantially lower threat to critical infrastructure than others; and, to impose a level of regulation that is consistent with the levels of risk posed.[157] RESA further cautioned that the imposition of the same costly burdens on both the utility and suppliers will have an unequal impact on the ability of suppliers to recover costs, because suppliers can only recover costs through the price of service to customers and, if costs are too high, suppliers could be forced to not offer competitive services.[158]

RESA also proposed that, if the PUC intends to impose any training requirements, it take a risk-based approach so that the levels of training, and the time and expense of the training, are commensurate with the level of risk any particular employee or class of employees pose on the system.[159] RESA urged caution regarding revisions to the existing regulations to ensure that: (1) they are in harmony with applicable federal and industry standards; and, (2) they recognize that this area of regulation is an ever moving target and thus use a flexible framework approach that can adapt as circumstances and

[155] NRG Comments at 2, RESA Comments at 1-2.
[156] RECA Comments at 2.
[157] *Id*.
[158] *Id*.
[159] RESA Comments at 2.

standards change without the need to revamp the entire structure.[160]

NRG stated that it does not support imposing new PUC-designed cybersecurity obligations on NGSs and EGSs for two overarching reasons: (1) an NGS or EGS which accesses and/or is in possession of personal information related to an electricity or gas customer is already subject to an existing subset of laws and regulations relating to data privacy, confidentiality, and cybersecurity, and additional regulations will not enhance or expand any cybersecurity benefit; and (2) as a commercial entity, an NGS or EGS must address cybersecurity and protection of personal information in order to successfully operate in the commercial marketplace, as well as to protect its own information assets.[161] NRG also notes that it is already regulated in its data security practices as a result of a myriad of federal and state laws, including Pennsylvania's Breach of Personal Information Notification Act. Additionally, NRG is required to comply with the PUC's regulations at 52 Pa. Code §§ 54.8 (EGS) and 62.78 (NGSs).[162] NRG asserted that it does not implement state-specific infrastructure, systems and networks, but instead achieves economies of scale to support its digital environment as well as to offer competitive products to customers while ensuring that such standards address compliance across many jurisdictions.[163] NRG provides an illustrative sampling of those state laws with which it currently must comply.[164]

NRG noted that the PUC has directed and significantly limited what customer information is made available through the Eligible Customer Lists of the utilities and that licensed EGSs and NGSs are required to comply with the PUC's privacy regulations at 52 Pa. Code §§ 54.8 (EGS) and 62.78 (NGSs) when in possession of such consumer

[160] *Id*.
[161] NRG Comments at 2-3.
[162] *Id*. at 4.
[163] *Id*. at 6-7.
[164] *Id*. at 7-10.

information.[165] NRG contended that "current regulatory obligations to maintain the confidentiality of the type of limited customer information the PUC permits an NGS or EGS to receive are sufficient to protect those elements of data and EGS or NGS is permitted to receive, and therefore adequately address risks associated with the loss of such data.[166]

NRG stated that, instead of increased regulation, the "PUC should pursue a public-private partnership to foster communication and collaboration and facilitate sharing of data security enhancements and exchange threat information.[167] Finally, NRG stated that it currently manages cybersecurity risks at all levels of its operations and that its commitment to cybersecurity is evidenced by its own training programs, information technology security team, third-party evaluations, corporate ethical standards, employee Code of Conduct, contractual relationships and insurance requirements.[168]

Verizon proposed that, to the extent there are entities regulated by the PUC that are not subject to Chapter 101's cybersecurity self-certification requirements, the PUC should monitor whether these entities become subject to the CISA and/or the Security Exchange Commission's regulations before it makes a determination of the necessity of bringing them under state regulation.[169] Verizon posited that, if information regarding the cybersecurity fitness, physical security, emergency response and/or business continuity plans of these entities is needed in the interim, the PUC has authority under 66 Pa.C.S. § 504 to request information. Finally, Verizon argued that, after the CISA regulations are final, "it might be appropriate to exempt certain entities from this PUC's process permanently, or even to eliminate the cybersecurity self-certification

[165] *Id*.
[166] *Id*.
[167] *Id*. at 14-15
[168] *Id*. at 16-28.
[169] Verizon Comments at 10.

altogether."[170]

In the Supplemental ANOPR, C&T Utilities added that all public utilities and competitive suppliers who serve Pennsylvania consumers in restructured industries be required to comply with reporting obligations that are appropriately tailored to represent situations of actual breach and harm to Pennsylvania consumers, unless the event has already been reported to another regulatory entity.[171] Columbia submitted that no public utility should be exempt from reporting cyber incidents to federal agencies, and incident reporting should also be applicable to suppliers and other entities subject to the Commission's oversight.[172]

Against this backdrop and with its proposed cybersecurity evaluations and programs regulations in front of stakeholders, the PUC invites further comment on whether it is appropriate or necessary for EGSs and NGSs to annually certify compliance with the corresponding subsections of Section 103.3 (relating to cybersecurity evaluations and programs).

G. Section 103.5. Waiver

In the introduction of our proposed Chapter 103, the PUC recognized that several of our jurisdictional public utilities have undertaken and maintain cybersecurity programs, plans, and standards that provide a reasonable level of fitness relative to their provision of service in the Commonwealth and that prescriptive regulations in these instances may not be in the public interest. Moreover, in the Supplemental ANOPR, the PUC solicited comment about whether public utilities should be allowed to request waiver for the use of cybersecurity programs and plans that utilize equal or stricter standards and frameworks.

---

[170] *Id*.
[171] C&T Utilities Comments at 8.
[172] Columbia Comments at 8.

1. Comments To The Supplemental ANOPR Relating To Waiver

A plurality of utilities answered in the affirmative. AT&T stated that if a utility is using a stricter standard than what the PUC has in place, then self-certification is appropriate.[173] FirstEnergy recommended that the PUC contemplate waivers for utility assets that are covered by other federal regulations, positing that this approach avoids duplicative or conflicting requirements.[174] Duquesne averred that enabling utilities to request these waivers encourages innovation and incentivizes utilities to adopt industry-leading best practices, while recommending conditions to the waivers including the utility's ability to map its framework to NIST CSF standards, demonstrate equivalent or better risk mitigation, and provide third-party validation or audit results.[175] PPL recommended that the PUC enable utilities to request waivers, while maintaining that Section 5.43 of the PUC's regulations already provides a clear path for utilities to request waivers of PUC regulations.[176] C&T Utilities noted their appreciation of the PUC's consideration of a waiver process for smaller utilities, and Aqua/Peoples stated that a waiver mechanism would allow the PUC to maintain oversight while recognizing the maturity and rigor of existing sector-specific frameworks.[177]

Three utilities suggested that a waiver process may not be necessary at all if a utility's standards are equal to or stricter than NIST CSF. Verizon contended that the PUC rules should have flexibility so that self-certification of cybersecurity programs that use equal or stricter standards than those the PUC enumerates would automatically qualify, rather than putting companies through the burden and expense of seeking a waiver.[178] PECO stated that waivers should not be necessary if a utility uses equal or stricter standards than NIST CSF.[179] Finally, PAWC suggested that in lieu of a waiver

[173] AT&T Comments at 8.
[174] FirstEnergy Comments at 4.
[175] Duquesne Comments at 6.
[176] PPL Comments at 4.
[177] C&T Utilities Comments at 6; Aqua/Peoples Comments at 4.
[178] Verizon Comments at 10.
[179] PECO Comments at 9.

requirement, the PUC include in its regulations a method by which the utility may aver that its cybersecurity programs use equal or stricter standards than the PUC's regulations require, and that such averment be acceptable by the PUC as proof of compliance.[180]

Columbia was the sole utility that said the PUC should not enable utilities to request waivers, arguing that allowing utilities to opt out of using a uniform framework risks undermining the consistency of federally recognized frameworks, while also noting that the PUC's staff may not have the requisite expertise to effectively manage enforcement for a variety of cybersecurity plans or frameworks.[181]

2. Comments To The Supplemental ANOPR Relating To Specific Criteria For Waiver

Moreover, the PUC asked for comment on whether it should specify criteria it would consider in a petition to waive the specific cybersecurity standards or framework it adopts. In response, the majority of utilities answered in the affirmative. AT&T and Aqua/Peoples both advocated for waivers when a utility proposes an alternative framework that may provide better protection, or when a utility can demonstrate strict adherence to equivalent or more rigorous cybersecurity frameworks.[182] PAWC stated that it was in favor of the PUC considering the use of a petition to allow a public utility to waive cybersecurity requirements.[183]

FirstEnergy recommended that the PUC specify bright-line criteria for how waivers would be evaluated, and that these criteria include how to handle overlapping federal regulations.[184] Duquesne also recommended that the PUC allow for a transparent and predictable waiver process, offering examples of outlined waiver criteria such as

[180] PAWC Comments at 4.
[181] Columbia Comments at 4.
[182] AT&T Comments at 8; Aqua/Peoples Comments at 4.
[183] PAWC Comments at 3.
[184] FirstEnergy Comments at 4.

demonstrated cybersecurity maturity or third-party certification, and risk assessments showing minimal exposure.[185] PECO recommended that the PUC clarify the criteria it may consider when reviewing a waiver petition, while Columbia argued that there should be a very specific and defined set of criteria to evaluate such petitions.[186]

Two utilities stated that they did not believe it necessary to specify waiver criteria. PPL stated that they did not believe specifying criteria to be necessary due to Section 5.43 of the PUC's regulations already setting forth the procedural and substantive requirements for utilities seeking a waiver of the PUC's regulations.[187] C&T Utilities stated that the current self-certification process is sufficient.[188] Verizon landed in the middle, stating that the language in the proposed Section 103.4 is reasonable in the context of the PUC's proposal but should be modified to include the possibility of waiving Section 103.2(d) for completeness.[189]

Thirdly, with respect to waiver, the PUC sought comment in the Supplemental ANOPR on whether to 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. Duquesne settled on a middle ground, cautioning that waivers from certain standards and frameworks should not be granted based on size alone; however, Duquesne posited that smaller utilities seeking a waiver must be able to show that certain controls are not relevant or feasible, and that their risk exposure is low.[190]

AT&T stated that they favored smaller utilities being able to opt out of inapplicable standards if they can certify that the risk is mitigated, while Columbia also

[185] Duquesne Comments at 6.
[186] PECO Comments at 9; Columbia Comments at 3.
[187] PPL Comments at 4.
[188] C&T Utilities Comments at 5.
[189] Verizon Comments at 9.
[190] Duquesne Comments at 7.

supported the PUC allowing waivers for utilities that do not serve critical facilities.[191] On the other end, PTA argued that continuing the current self-certification process utilized by the PUC obviates the need for any changes in this area, and PAWC stated their belief that the PUC should establish basic standards that apply to all utilities regardless of size, while also recommending that utilities have more than three months to implement any new standards.[192]

C&T Utilities noted that for many regulatory requirements, filing a petition for a waiver is an efficient method to accommodate smaller utility risks and resources; however, they urged the PUC to also adjust the appropriate placement of smaller utilities with no critical infrastructure within the proposed compliance classes.[193] Specifically, they aver that a utility serving less than 100,000 customers which does not have bulk electric system assets and/or other critical infrastructure under federal definitions should be classified as a Class 3 utility, which will enable the PUC to use Class 2 requirements for smaller utilities with heightened risks while maintaining appropriate Class 3 oversight for smaller utilities that do not have those facilities.[194]

Verizon noted that the absence of applicable federal or industry standards might be a factor that requires greater PUC involvement in smaller companies' cybersecurity practices.[195] PB Transport recommended that the PUC's rulemaking incorporate provisions to assist smaller utilities in meeting self-certification requirements, to enhance compliance while avoiding disproportionate costs.[196]

[191] AT&T Comments at 9; Columbia Comments at 4.
[192] PTA Comments at 2; PAWC Comments at 5.
[193] C&T Utilities Comments at 6.
[194] *Id.*
[195] Verizon Comments at 10.
[196] PB Transport Comments at 2.

3. The PUC Invites Comments On Section 103.5

Upon review of all the comments received about waiver, the PUC's proposed regulations provide an opportunity for jurisdictional public utilities to petition for waiver of the requirements in Section 103.3 based on meeting specific criteria set forth in Section 103.5(a). The PUC seeks comments on the scope of its proposed waiver and on whether the criteria provided needs greater specificity. The PUC has attempted to accommodate jurisdictional public utilities with small customer bases and limited critical infrastructure with the creation of the class system by size but seeks comment on whether the proposed waiver provision should be expanded to more fully consider hardships these utilities may encounter in attempting to comply with Section 103.3.

H. Section 103.6. Accounting For Changes And Updates To External Reference And Standards

Even as the PUC proposed to require utility classes 1-4 to adhere to the NIST CSF and additional requirements, it recognizes that these frameworks and the Special Publications named directly will be updated and amended. To account for how such changes will be incorporated into Chapter 103, in Section 103.6 the PUC proposes procedures it will follow to allow public input prior to such changes becoming effective in the Commonwealth for jurisdictional public utilities, including publishing notice in the *Pennsylvania Bulletin*. The PUC seeks comments on these proposed procedures.

I. Section 103.7. Compliance

In the Supplemental ANOPR, the PUC asked public utilities how it should enforce the requirements in the event of violations. AT&T and Duquesne both stated that they believe the current enforcement tools are adequate and do not require modification.[197] Verizon recommended that the Commission defer to federal authorities with regard to

[197] AT&T Comments at 9; Duquesne Comments at 8.

substantive issues and rely on its normal processes for procedural issues.[198]

PECO recommended that the Commission adopt an enforcement framework that prioritizes remediation of identified vulnerabilities over compliance administration and civil penalties.[199] Columbia argued that the PUC's Bureau of Investigation and Enforcement (I&E) should leverage the existing regulatory framework that allows filing a formal complaint to prosecute any violation of the Code, and that any penalties proposed by I&E be subject to review under the *Rosi* standards.[200]

In its proposed Section 103.7, the PUC authorizes review of public utilities' compliance certifications, as well as the underlying cybersecurity plans and programs, and clarifies that public utility compliance with cybersecurity requirements may be examined by the PUC at any point in activities like the established management audit process. As Columbia's comments make clear, violations uncovered through this process could lead to the filing of a formal complaint by I&E.

VII. Proposed Chapter 104 Relating To Cybersecurity Evaluations, Programs, Standards, And Plans

Consistent with its recommended removal of cybersecurity accident reporting requirements from Sections 57.11, 59.11, 61.11, and 65.2 of its regulations, as discussed above in Section IV of this Order, the PUC proposes a new chapter, Chapter 104 (re Cybersecurity Incident Reporting), to address incident reporting requirements. Chapter 104 identifies implicitly the role and scope the PUC presently ascertains for itself with respect to reporting, provides definitions pertinent to cyber incident reporting, and states the instances and information that a public utility must report.

---

[198] Verizon Comments at 11.
[199] PECO Comments at 11.
[200] Columbia Comments at 5 (*Rosi* refers to *Rosi Pa. P.U.C. v. NCIC Operator Services*, M-00001440 (Order entered December 21, 2000).).

The PUC seeks additional informed stakeholder comment on the role it establishes for itself regarding cybersecurity incident reporting, as well as sections 104.1-104.2 below.

A. The Role Of The PUC In Cyber Incident Reporting

In discerning the scope of its role in incident reporting, in its Supplemental ANOPR the PUC solicited comments from stakeholders related to the following areas:

a. Trend and threat analysis;
b. Vulnerability and mitigation assessment;
c. The provision of early warnings;
d. Incident response and mitigation;
e. Supporting Federal efforts to disrupt threat actors and advancing cyber resiliency;
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.

Supplemental ANOPR at Annex A.

1. Comments To The Supplemental ANOPR Related To The Scope Of The PUC's Role In Cyber Incident Reporting

In general, AT&T stated that the PUC has the option to subscribe to and redistribute relevant Information Sharing and Analysis Center (ISAC) information; AT&T further stated that the PUC should share threat information with CISA, the FBI, sector ISACs, or others as appropriate, and coordinate with PEMA when requested.[201] Duquesne stated that for areas (a) through (d) (relating to trend and threat analysis; vulnerability and mitigation assessment; provision of early warnings; and incident response and mitigation), it opined no additional involvement by the PUC was necessary, stating that resources such as NERC's Electronic Information Sharing and Analysis

[201] AT&T Comments at 12.

Center (E-ISAC), Infraguard, the FBI, and DHS Cybersecurity and Infrastructure Security Agency already effectively provide this information-sharing function.[202] Duquesne stated that the PUC should amplify those existing avenues to regulated entities.[203]

PPL did not have specific responses to each of the subparts, but stated its general agreement that the PUC should play a vital role in utility cybersecurity oversight.[204] PPL further recommended that the PUC continue to collaborate with federal agencies to ensure the sharing of cyber and threat intelligence, particularly as related to critical infrastructure, and recognized the unique role that the PUC can play in providing public utilities with the insight and tools necessary to identify and assess cybersecurity risk and trends and to help the industry improve incident response and mitigation.[205] C&T Utilities stated support for the PUC's roles in items (c), (d), and (f) (related to provision of early warnings; incident response and mitigation; and sharing cybersecurity threat and incident information with stakeholders), but stated that they did not support the roles in the list that would duplicate federal and law enforcement efforts.[206] Columbia offered that the PUC can provide customers with the most protection against cybersecurity attacks through proper policies and rate structures that encourage jurisdictional utilities to identify, protect, detect, respond, and recover from attacks; they further encouraged the PUC to implement alternative recovery mechanisms to support timely implementation of cybersecurity measures.[207]

[202] Duquesne Comments at 10.
[203] *Id.*
[204] PPL Comments at 7.
[205] *Id.*
[206] C&T Utilities Comments at 8.
[207] Columbia Comments at 6.

Upon review of the submitted comments directed to areas (a)-(f) above, the PUC determines that its role in cyber incident reporting relates to areas (e) and (f), which it addresses in this Order.

2. Comments To The Supplemental ANOPR Related To The PUC Supporting Federal Efforts To Disrupt Threat Actors And Advance Cyber Resiliency

The PUC's Supplemental ANOPR asked commenters to identify the role of the PUC in supporting federal efforts to disrupt threat actors, as well as advancing cyber resiliency.[208] In response, Verizon suggested that no action is required by the PUC with respect to supporting federal efforts to disrupt threat actors.[209] PTA stated that the PUC's ongoing multi-agency and industry stakeholder efforts with the Black Sky Steering Committee (BSSC) make the BSSC the ideal forum in which to discuss cybersecurity threats and share information from federal and state agencies to help identify and mitigate cyber threats.[210]

FirstEnergy stated that this task is already well-established by the commercial security industry at cost-effective pricing through various sector-specific security organizations, and averred that the PUC establishing its own capability would be duplicative and not cost-effective for the Commonwealth; further, FirstEnergy opposed the use of "cyber incident data" in the furtherance of cybersecurity research because such information is already widely available and at-scale such that the risk of accidental sharing of confidential information through a research program is much more of a concern than the availability of the data in general.[211] Duquesne recommended that the PUC support federal cybersecurity efforts by fostering collaboration with agencies like DHS and the FBI, promoting best practices, and encouraging utilities to share

[208] Supplemental ANOPR, Appendix A.
[209] Verizon Comments at 15.
[210] PTA Comments at 2.
[211] FirstEnergy Comments at 8.

anonymized incident data for research; additionally, Duquesne recommended that the PUC engage with software and equipment vendors to address vulnerabilities and align state regulations with evolving federal standards.[212]

PECO recommended that the PUC 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.[213] C&T Utilities stated that they do not support roles that would duplicate federal and law enforcement efforts.[214] PAWC stated that they do not see a role for the PUC in incident response and mitigation.[215] Aqua/Peoples recommended that the PUC's role relate to supporting federal resilience efforts.[216] EAP averred that supporting federal resilience efforts is an appropriate role for the PUC.[217] Columbia stated that this function is already being performed by the federal government, and that the PUC does not need to duplicate efforts.[218]

3. Comments To The Supplemental ANOPR Related To The PUC Sharing Cybersecurity Threat And Incident Information With Public Utility, State, And Federal Stakeholders

The PUC also solicited comments about the role it had to play in 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 potential risk to the consumer's health, safety, and/or welfare. .[219]

[212] Duquesne Comments at 11.
[213] PECO Comments at 19.
[214] C&T Utilities Comments at 8.
[215] PAWC Comments at 8.
[216] Aqua/Peoples Comments at 7.
[217] EAP Comments at 7.
[218] Columbia Comments at 8.
[219] Supplemental ANOPR, Appendix A.

Verizon suggested that no action is required by the PUC but stated that the PUC should become aware of specific cybersecurity threat information of this nature and share it with parties at risk.[220] PTA stated that the PUC's ongoing multi-agency and industry stakeholder efforts with the Black Sky Steering Committee make the Committee the ideal forum in which to discuss cybersecurity threats and share information from federal and state agencies to help identify and mitigate cyber threats.[221]

FirstEnergy stated that this task is already well-established by the commercial security industry at cost-effective pricing through various sector-specific security organizations and through industry partnerships.[222] PECO recommended that the PUC share unique information that they possess with all stakeholders to ensure a complete response by industry members; they further recommended that, if the PUC receives information through confidential means, the PUC 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.[223] C&T Utilities stated their support for the PUC's role in sharing cybersecurity threat and incident information among shareholders.[224] PAWC stated their belief that the PUC can and should play a role in disseminating information related to cyber incidents and threat data.[225]

Aqua/Peoples recommended that the PUC's role relates to sharing information among stakeholders; they also noted that there are already several federal regulatory frameworks in place that address cybersecurity regulation, and recommended that the PUC defer to the existing federal framework which is better suited to sector-specific federal agencies.[226] EAP averred that information sharing among stakeholders is an

[220] Verizon Comments at 16.
[221] PTA Comments at 2.
[222] FirstEnergy Comments at 8.
[223] PECO Comments at 19-20.
[224] C&T Utilities Comments at 8.
[225] PAWC Comments at 8.
[226] Aqua/Peoples Comments at 7.

appropriate role for the PUC.[227] Columbia stated that this function is already being performed by the federal government and the PUC does not need to duplicate efforts.[228]

With these comments considered, the PUC proposes Chapter 104 with the understanding that it plays a significant role in facilitating information sharing between entities that gather cybersecurity incident information and the public utilities that require access to such information.

B. Chapter 104.1. Definitions

Section 104.1 provides definitions of cybersecurity terms the PUC proposes to use in requiring jurisdictional public utilities to comply with Section 104.2 (relating to reporting requirements). These definitions were primarily drawn from the NIST CSRC glossary.[229] The definitions of these terms may have been modified by the PUC from several offerings or uses to best serve the purposes of our cybersecurity regulations.

Additionally, the PUC provides a definition for "public utility," which reflects Section 102 of the Public Utility Code (Code), 66 Pa.C.S. § 102. In our Supplemental ANOPR, the PUC sought comment on whether specific types of public utilities should be exempt from reporting cyber incidents.

Three utilities stated their support for exempting specific types of public utilities from reporting cyber incidents. AT&T averred that telecommunications providers should continue to be exempt from reporting incidents to the Commission.[230] Verizon advocated that communications companies regulated by the Commission should be exempt from any new requirement to report cyber incidents, as proposed in Chapter 104, and pointed

[227] EAP Comments at 7.
[228] Columbia Comments at 8.
[229] The NIST CSRC glossary can be found at https://csrc.nist.gov/glossary (last accessed [date]).
[230] AT&T Comments at 12.

to Chapter 30 of the Code as a limit on the Commission's authority to impose new reporting requirements on such companies.[231] Verizon averred that it would continue to be subject to the Commission's rules at 52 Pa. Code § 67.1, and noted that the Commission recognized the limitations in Chapter 30 in its revisions to Section 67.1 in 2011.[232] Verizon went on to state that new reporting requirements are not necessary for the communications sector, which is already subject to reporting and other requirements from various federal agencies.[233] EAP recommended that utilities with no critical infrastructure or those subject to comprehensive federal regulation should be exempt from duplicative reporting.[234]

The remainder of the utilities who answered this question were either against any exemptions or found a middle ground. FirstEnergy recommended that all public utilities be required to report significant cybersecurity incidents to the Commission where the incident impacts delivery of utility service or requires notification to the Pennsylvania Attorney General under the state's breach notification law.[235] PPL stated that they do not support exempting certain types of fixed public utilities from the requirement to report cyber incidents, as a cyber incident could impact critical infrastructure not isolated to one utility or type of utility; as such, to the extent reporting is required, PPL recommended that all fixed utilities be required to report cyber incidents.[236]

Duquesne recommended that certain types of public utilities could be considered for exemption from cyber incident reporting if they pose minimal risk to critical infrastructure, have limited digital exposure, or serve a very small customer base; however, they recommended that any exemption be carefully evaluated to ensure it does

[231] Verizon Comments at 16.
[232] *Id.* at 16-17.
[233] *Id.* at 18.
[234] EAP Comments at 7-8.
[235] FirstEnergy Comments at 9.
[236] PPL Comments at 8.

not create blind spots in the state's overall cybersecurity posture, especially as even small utilities can be entry points for broader attacks.[237] Duquesne further recommended that the process for exemptions be transparent and clearly articulated.[238]

Based on these comments, the PUC proposes to exempt public utilities defined in subsection (1)(vi) of Section 102 of the Code, "any person or corporations now or hereafter owning or operating in this Commonwealth equipment or facilities for conveying or transmitting messages or communications, except as set forth in paragraph (2)(iv), by telephone or telegraph or domestic public land mobile radio service including, but not limited to, point-to-point microwave radio service for the public for compensation." These communications providers are not subject to the PUC's current cyber accident reporting regulations pursuant to the limitations of 66 Pa.C.S. § 3015(e)-(f), precluding the PUC from adding new reporting requirements to these providers except in limited situations.[239] Thus, communications providers have the option of filing required service outage reporting consistent with Section 67.1 or the comparable FCC report as long as it contains, at minimum, the information required under subsections 67.1(b)(1), (3), (6), (7), (11), and (13).[240]

The PUC seeks comment on all of its proposed definitions but specifically solicits additional comment on its proposal to continue exempting communications providers from the specific reporting requirements of Section 104.2 in light of Chapter 30 of the Code and Section 67.1 of the PUC's current regulations.

---

[237] Duquesne Comments at 11.
[238] *Id.*
[239] *See Proposed Rulemaking for Revision of 52 Pa. Code Chapters 57, 59, 65 and 67 Pertaining to Utilities' Service Outage Response and Restoration Practices*, Docket No. L-2009-2104274, Final Rulemaking Order at 6, 27 (entered September 23, 2011) ("As to Verizon's comments regarding the application of the reporting requirements to telephone companies, we agree with the comments and revised the section to accurately reflect them. As discussed in the general comments section to this final rulemaking order, the Commission did not add to or change any of the current reporting requirements for telephone companies.)
[240] *Id.* at 27.

C. 52 Pa. Code Section 104.2. Reporting Requirements

Section 104.2 proposes the cybersecurity incidents that public utilities must report to the PUC, as well as the time frame and pertinent information for such reporting. These cyber incidents include those that arise on the network of a public utility or on the network of a third-party connected to or relied on by the utility which causes certain outcomes, as well as incidents involving ransomware. The PUC seeks informed comment on the cyber incidents for which we propose to require reporting as well as the time frame to report after the discovery of a cyber incident.

Additionally, in our Supplemental ANOPR, the PUC asked public utilities whether it should accept incident reports submitted by a utility to comply with another agency's regulations.

AT&T stated that there are already rules in place governing the reporting of network outages to the PUC; thus, AT&T averred that there is no reason for the PUC to obtain copies of incident ("substantial") reports.[241] Verizon maintained that the PUC should not require cyber incident reporting from communications provider, pointing to Section 67.1 of the PUC's regulations for existing requirements, and, once again, identified the preclusions of Chapter 30 to limit the PUC's ability to impose new reporting requirements.[242] Duquesne averred that cybersecurity incident reporting is already robust and recommended that the PUC avoid adding to that burden and instead be open to receiving a copy of a standardized report form, such as the DOE Electric Emergency Incident and Disturbance Report (DOE-417) form; Duquesne further recommended that if information reported to another agency is not pertinent to the PUC, the utility be permitted to redact sensitive information.[243]

[241] AT&T Comments at 14.
[242] Verizon Comments at 19.
[243] Duquesne Comments at 12.

FirstEnergy averred that to be effective, cyber information reporting must require the correct amount of specificity to avoid unrealistic and burdensome reporting requirements that will not ultimately provide regulators with the relevant information necessary to stay appraised of malicious breaches to the system; FirstEnergy further noted that it could be helpful and more efficient if the PUC permitted utilities to send a copy of cybersecurity incident reports submitted to other regulatory agencies to satisfy the reporting requirement.[244] PPL recommended that the PUC collaborate with other agencies to prevent the creation of overlapping, burdensome, or different reporting requirements; in order to do so, PPL recommended that the PUC collaborate with other agencies imposing cyber reporting requirements or take those requirements into consideration when developing its own standards in order to reduce regulatory overlap.[245]

FirstEnergy also encouraged the Commission to remove language in Chapter 104.2(a)(iv) regarding "potential compromise," as a jurisdictional utility is not in a position to determine if its risk or incident is a risk to any other entity, and such assessments require access to information and visibility beyond a utility's control—thus, such assessments are more appropriately conducted by federal or state agencies with greater authority and visibility.[246]

PECO averred that the PUC and public utilities could save administrative resources if the PUC accepts incident reports generated in response to federal cyber incident reporting regulations from those utilities subject to them, and recommended that the PUC coordinate secure access to DOE and DHS's web portals, or absent this access, accept incident forms generated by federal portals; PECO averred that these incident reports will give the PUC the information it seeks with respect to cyber incidents that impact operations or customer information.[247] PECO noted that utilities are already

[244] FirstEnergy Comments at 9.
[245] PPL Comments at 8.
[246] *Id.* at 15-16.
[247] PECO Comments at 20.

subject to multiple cyber incident reporting laws and expectations, and recommended that the PUC allow cyber incident reports generated for federal agencies to satisfy PUC cyber incident reporting requirements where possible.[248] C&T Utilities did not have a position on this item.[249] EAP recommended that the PUC accept reports submitted to TSA, DOE, or CISA to satisfy its requirements where applicable.[250]

Columbia did not recommend a requirement to report incidents at the state level in addition to required reporting at the federal level.[251] Columbia opined that if the PUC does take this step, then the PUC should accept incident reports that comply with another agency's regulations and suggested that the PUC establish a means by which the federal agency automatically notifies the PUC when a company under its jurisdiction reports a cyber incident.[252] PAWC stated their belief that there is value in allowing the PUC to accept reports submitted by a utility to comply with another agency's regulations.[253] Aqua/Peoples recommended that the PUC accept cyber incident reports submitted to federal agencies to satisfy its requirements where applicable; they further recommended that all cybersecurity documents remain as confidential security information and not be filed with or stored at the PUC due to security risks; instead, they recommended the PUC staff conduct on-site reviews at public utility facilities under appropriate confidentiality agreements.[254]

In light of these comments, the PUC proposes in subsection (d) to accept cybersecurity incidents reports that public utilities submit to federal or other state agencies where such reports are sufficient to meet the PUC's purposes. The PUC seeks additional comment on this proposal.

---

[248] *Id.*
[249] C&T Utilities Comments at 9.
[250] EAP Comments at 7.
[251] Columbia Comments at 8.
[252] *Id.* at 9.
[253] PAWC Comments at 9.
[254] Aqua/Peoples Comments at 7-8.

CONCLUSION

Accordingly, under sections 331, 501, 504, 505, 506, and 1501 of the Public Utility Code (66 Pa.C.S. §§ 331, 501, 504-506, and 1501; sections 201 and 202 of the Act of July 31, 1968 (P.L. 769, No. 240), referred to as the Commonwealth Documents Law (45 P.S. §§ 1201 and 1202), and the regulations promulgated thereunder at 1 Pa. Code §§ 7.1, 7.2, and 7.5 (relating to notice of proposed rulemaking required: adoption of regulations; and approval as to legality); section 204(b) of the Commonwealth Attorneys Act (71 P.S. § 732-204(b)); section 5 of the Regulatory Review Act (71 P.S. § 745.5); and section 612 of The Administrative Code of 1929 (71 P.S. § 232), and the regulations promulgated thereunder at 4 Pa. Code §§ 7.231—7.234 (relating to fiscal note), we are considering adopting proposed changes to existing regulations and proposed new regulations, at 52 Pa. Code §§ 57.11, 59.11, 61.11, 61.45, 65.2, 101.1-101.7, 103.1-103.7, 104.1-104.2, as described below and proposed in Annex A.; **THEREFORE,**

IT IS ORDERED:

1. That a proposed rulemaking be opened to consider the proposed amendments to 52 Pa. Code §§57.11 (relating to accident reporting for electricity public utilities), 59.11 (relating to accident reporting for gas public utilities), 61.11 (relating to accident reporting for steam utilities), 61.45 (relating to security planning and emergency contact lists for steam heating service), and 65.2 (relating to accident reporting for water public utilities), Chapter 101 (relating to public utility preparedness through self certification), as well as adding new chapters 103 (relating to cybersecurity evaluations, programs, standards, and plans) and 104 (relating to cybersecurity incident reporting), as described below and set forth in Annex A.

2. That a copy of this Notice of Proposed Rulemaking Order shall be posted on the Public Utility Commission's website at Docket No. L-2022-3034353.

3. That this Notice of Proposed Rulemaking shall be served on all public utilities enrolled in the Public Utility Commission's e-Filing system and that a Secretarial Letter providing notice of this proceeding shall be served by mail on all motor vehicle carriers.

4. That the Law Bureau shall deposit this Notice of Proposed Rulemaking Order with the Legislative Reference Bureau to be published in the *Pennsylvania Bulletin.*

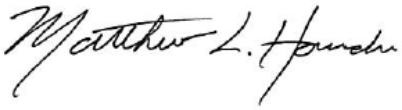
5. That interested parties may submit written comments, referencing Docket No. L-2022-3034353, within 90 days from the date this Notice of Proposed Rulemaking Order is published in the *Pennsylvania Bulletin*. Written reply comments may be filed during the 45-day period following the 90-day period for filing written comments. Comments may be filed either through the Public Utility Commission's e-Filing system or by mail. Comments filed during the Public Comment Period will be posted to the Public Utility Commission's website and forwarded by the Public Utility Commission to the majority and minority chairs of the Senate Consumer Protection and Professional Licensure Committee and the House Consumer Protection, Technology, and Utilities Committee and to the Independent Regulatory Review Commission.

6. Parties to proceedings pending before the Public Utility Commission may open and use an e-filing account through the Commission's website, or you may submit your filing by overnight delivery. If a filing contains confidential or proprietary material, the filing must be submitted by overnight delivery. Filing information can be found on the Commission's website at https://www.puc.pa.gov/filing-resources/efiling/.

7. That comments filed prior to publication of the *Notice of Proposed Rulemaking* in the *Pennsylvania Bulletin* will be considered untimely filed and may be rejected by the Pennsylvania Public Utility Commission.

8. That the contact persons for this proceeding are Colin W. Scott, Esq., Law Bureau, 717-783-5949, colinscott@pa.gov; Stephanie A. Wilson, Esq., Law Bureau, 717-787-1859, stepwilson@pa.gov, Michael Holko, Director, Office of Cybersecurity Compliance and Oversight, (717) 425-5327, miholko@pa.gov, Daniel Searfoorce, Manager—Water, Reliability and Emergency Preparedness Division, Bureau of Technical Utilities Services, (717) 783-6159, dsearfoorc@pa.gov, and Karen Thorne, Regulatory Review Assistant, Law Bureau, kathorne@pa.gov.

BY THE COMMISSION



Matthew L. Homsher
Secretary

(SEAL)

ORDER ADOPTED: June 18, 2026

ORDER ENTERED: June 24, 2026

Cyber Security NOPR

Annex A

§ 57.11. Accidents.

(a) *General.* A public utility shall submit a report of each reportable accident involving the facilities or operations of the public utility in this Commonwealth to the Secretary of the Commission.

(b) *Reportable accidents.* Reportable accidents are those involving **public** utility facilities or operations which result in one or more of the following circumstances:

(1) The death of a person.

(2) Injury to a person sufficient that the injured person requires immediate treatment at a hospital emergency room or in-patient admittance to a hospital, or both.

(3) An occurrence of an unusual nature, whether or not death or injury of a person results, which apparently will result in a prolonged and serious interruption of normal service.

(4) An occurrence of an unusual nature that is a physical **[or cyber]** attack**[, including attempts against cyber security measures as defined in Chapter 101 (relating to public utility preparedness through self certification)]** that causes an interruption of service or over $50,000 in damages, or both.

(c) *Exceptions.* Injuries, as defined in subsection (b)(1) and (2), may not include those suffered as a result of a motor vehicle accident with **public** utility facilities unless on or both of the following circumstances apply:

(1) A vehicle involved in the accident is owned by the **public** utility or driven by a **public** utility employee while on duty.

(2) Some or all of the injuries were as a result of contact with electrified facilities.

(d) *Telephone reports.* A report by telephone shall be made immediately after the **public** utility becomes aware of the occurrence of a reportable accident under subsection (b)(1), (3) or (4). A report by telephone **shall** be made within 24 hours after a **public** utility becomes aware of a reportable accident under subsection (b)(2).

(e) *Written reports.* A written report shall be made on Form UCTA-8 within 30 days of the occurrence of a reportable accident. For reportable accidents under subsection (b)(4), a **public** utility **[may] shall** remove from Form UCTA-8 information that would compromise the security of the utility or hinder an active criminal investigation. Accidents reportable on forms required by the Bureau of Workers' Compensation, Department of Labor and Industry, or the United States Department of Energy, may be reported to the Commission by filing a copy of the forms in lieu of a report on Form

UCTA-8, as long as the alternative forms, at a minimum, provide the following information:

(1) The **public** utility name.

(2) The date of reportable accident.

(3) The date of report.

(4) The location where the reportable accident occurred.

(5) The name, age, residence and occupation of the injured or deceased parties.

(6) The general description of the reportable accident.

(7) The name and telephone number of the reporting officer.

(f) *Form availability.* Blank UCTA-8 forms are available for download on the Commission's web site.

(g) *Reports not exclusive.* The reporting under this chapter is not limited to the requirements in this section and does not limit requests for additional information.

§ 59.11. Accidents.

(a) *General.* Each public utility shall submit a report of each reportable accident involving the facilities or operations of the public utility in this Commonwealth as provided in this section. The reports shall be addressed to the Secretary of the Commission.

(b) *Reportable accidents.* Reportable accidents are those involving **public** utility facilities or operations which result in one or more of the following circumstances:

(1) The death of a person.

(2) Injury to a person sufficient that the injured person requires immediate treatment at a hospital emergency room or in-patient admittance to a hospital, or both.

(3) An event that involves a release of **natural** gas from a pipeline or of LNG or gas from an LNG facility, which results in estimated property damage, including the cost of **natural** gas lost of the operator or others, of at least $50,000 in market value.

(4) An event that results in an emergency shutdown of an LNG facility.

(5) An occurrence of an unusual nature that is a physical **[or cyber]** attack**[, including attempts against cyber security measures as defined in Chapter 101 (relating to public utility preparedness through self certification)]** which causes an interruption of service or over $50,000 in damages, or both.

(c) *Exceptions.* Injuries, as defined in subsection (b)(1) and (2), may not include those suffered as a result of a motor vehicle accident with **public** utility facilities unless one or both of the following circumstances apply:

(1) A vehicle involved in the accident is owned by the **public** utility or driven by a **public** utility employee while on duty.

(2) Some or all of the injuries were as a result of contact with natural gas facilities transporting or storing natural gas or due to gas escaping from natural gas facilities.

(d) *Telephone reports.* A report by telephone shall be made immediately after the **public** utility becomes aware of the occurrence of a reportable accident under subsection (b)(1), (3), (4) and (5). A report by telephone shall be made within 24 hours after the **public** utility becomes aware of a reportable accident under subsection (b)(2).

(e) *Written reports.* A written report shall be made on Form UCTA-8 within 30 days of the occurrence of a reportable accident. For reportable accidents under subsection (b)(5), a **public** utility shall remove from Form UCTA-8 information that would compromise the security of the **public** utility or hinder an active criminal investigation. Accidents reportable on forms required by the Bureau of Workers' Compensation, Department of

Labor and Industry, or the United States Department of Transportation, Pipeline and Hazardous Materials Safety Administration, may be reported to the Commission by filing a copy of the forms in lieu of a report on Form UCTA-8, as long as the alternative forms, at a minimum, provide the following information:

(1) The **public** utility name.

(2) The date of the reportable accident.

(3) The date of the report.

(4) The location where the reportable accident occurred.

(5) The name, age, residence and occupation of the injured or deceased parties.

(6) The general description of the reportable accident.

(7) The name and telephone number of the reporting officer.

(f) *Form availability.* Blank UCTA-8 forms are available for download on the Commission's web site.

(g) *Reports not exclusive.* The reporting under this chapter is not limited to the requirements in this section and does not limit requests for additional information.

§ 61.11. Accidents.

(a) *General.* A steam utility shall submit a report of each reportable accident involving the facilities or operations of the steam utility in this Commonwealth. The reports shall be addressed to the Secretary of the Commission.

(b) *Reportable accidents.* Reportable accidents are those involving steam utility facilities or operations which result in one or more of the following circumstances:

(1) The death of a person.

(2) Injury to a person sufficient that the injured person requires immediate treatment at a hospital emergency room or in-patient admittance to a hospital, or both.

(3) An event that involves a release of steam from the steam utility, which results in estimated property damage of at least $50,000.

(4) An occurrence of an unusual nature, whether or not death or injury of a person results, which apparently will result in a prolonged and serious interruption of normal service.

(5) An event that results in an emergency shutdown of the steam utility.

(6) An occurrence of an unusual nature that is a physical **[or cyber-]**attack**[, including an attempt to interfere with a steam utility's computers, software and communication networks that support, operate or otherwise interact with the steam utility's operation]**.

(7) An unusual occurrence that is significant in the judgment of the steam utility.

(c) *Exception.* Injuries, as defined in subsection (b)(1) and (2), may not include those suffered as a result of a motor vehicle accident with **public** utility facilities unless a vehicle involved in the accident is owned by the steam utility or driven by a **public** utility employee while on duty.

(d) *Telephone reports.* A report by telephone shall be made immediately to the Commission's Pipeline Safety Division after the steam utility becomes aware of an occurrence of a reportable accident under subsection (b)(1), (3), (4) or (5). A report by telephone shall be made within 24 hours after the steam utility becomes aware of a reportable accident under subsection (b)(2).

(e) *Written reports.* A written report shall be made on Form UCTA-8 within 30 days of the occurrence of a reportable accident. For reportable accidents under subsection (b)(6), a steam utility shall remove from Form UCTA-8 information that would compromise the security of the **public** utility or hinder an active criminal investigation. Accidents reportable on forms required by the Bureau of Workers' Compensation, Department of

Labor and Industry, or the United States Department of Transportation, Pipeline and Hazardous Materials Safety Administration, shall be reported to the Commission by filing a copy of the forms instead of a report on Form UCTA-8, as long as the alternative forms, at a minimum, provide all of the following information:

(1) The name of the steam utility.

(2) The date of the reportable accident.

(3) The date of the report.

(4) The location where the reportable accident occurred.

(5) The name, age, residence and occupation of the injured or deceased parties.

(6) The general description of the reportable accident.

(7) The name and telephone number of the reporting officer.

(f) *Form availability.* Blank UCTA-8 forms are available for download on the Commission's web site.

(g) *Reports not exclusive.* The reporting under this chapter is not limited to the requirements in this section and does not limit requests for additional information.

§ 61.45. Security planning and emergency contact list.

(a) A steam utility shall develop and maintain written plans for physical **[and cyber]** security, emergency response and business continuity in accordance with § 101.3 (relating to plan requirements).

§ 65.2. Accidents.

(a) *General.* A public utility shall submit a report of each reportable accident involving the facilities or operations of the public utility in this Commonwealth. The reports shall be addressed to the Secretary of the Commission.

(b) *Reportable accidents.* Reportable accidents are those involving **public** utility facilities or operations which result in one or more of the following circumstances:

(1) The death of a person.

(2) Injury to a person sufficient that the injured person requires immediate treatment at a hospital emergency room or in-patient admittance to a hospital, or both.

(3) An occurrence of an unusual nature, whether or not death or injury of a person results, which apparently will result in a prolonged and serious interruption of normal service.

(4) An occurrence of an unusual nature that is a physical **[or cyber]** attack**[, including attempts against cyber security measures as defined in Chapter 101 (relating to public utility preparedness through self certification)]** which causes an interruption of service or over $50,000 in damages, or both.

(c) *Exceptions.* Injuries, as defined in subsection (b)(1) and (2), may not include those suffered as a result of a motor vehicle accident with **public** utility facilities unless one or both of the following circumstances apply:

(1) A vehicle involved in the accident is owned by the **public** utility or driven by a **public** utility employee while on duty.

(2) Some or all of the injuries were as a result of contact with water facilities transporting or storing water or due to water escaping from water facilities.

(d) *Telephone reports.* A report by telephone shall be made immediately after the **public** utility becomes aware of the occurrence of a reportable accident under subsection (b)(1), (3) and (4). A report by telephone shall be made within 24 hours after a **public** utility becomes aware of a reportable accident under subsection (b)(2).

(e) *Written reports.* A written report shall be made on Form UCTA-8 within 30 days of the occurrence of a reportable accident. For reportable accidents under subsection (b)(4), the **public** utility **[may] shall** remove from Form UCTA-8 information that would compromise the security of the **public** utility or hinder an active criminal investigation. Accidents reportable on forms required by the Bureau of Workers' Compensation, Department of Labor and Industry, Department of Environmental Protection or the United States Environmental Protection Agency may be reported to the Commission by

filing a copy of the forms in lieu of a report on Form UCTA-8, as long as the alternative forms, at a minimum, provide the following information:

(1) The **public** utility name.

(2) The date of reportable accident.

(3) The date of report.

(4) The location where the reportable accident occurred.

(5) The name, age, residence and occupation of the injured or deceased parties.

(6) The general description of the reportable accident.

(7) The name and telephone number of the reporting officer.

(f) *Form availability.* Blank UCTA-8 forms are available for download on the Commission's web site.

(g) *Reports not exclusive.* The reporting under this chapter is not limited to the requirements in this section and does not limit requests for additional information.

CHAPTER 101. PUBLIC UTILITY PREPAREDNESS **[THROUGH SELF CERTIFICATION]**

Sec.

§ 101.1. Purpose.

This chapter requires a jurisdictional utility to develop and maintain appropriate written physical security, **[cyber security,]** emergency response and business continuity plans to protect this Commonwealth's infrastructure and ensure safe, continuous and reliable utility service. **[A jurisdictional utility shall submit a Self Certification Form to the Commission documenting compliance with this chapter.]**

§ 101.2. Definitions.

The following words and terms, when used in this chapter, have the following meanings, unless the context clearly indicates otherwise:

Abnormal operating condition—A condition possibly showing a malfunction of a component or deviation from normal operations that may **result in both**:

(i) **[Indicate]An indication of** a condition exceeding design limits.

(ii) **[Result in a] A** hazard to person, property or the environment.

Business continuity plan—A written plan that will ensure the continuity or uninterrupted provision of operations and services through arrangements and procedures that enable a utility to respond to an event that could occur by abnormal operating conditions.

Business recovery—The process of planning for and implementing expanded operations to address less time-sensitive business operations immediately following an abnormal operating condition.

Business resumption—The process of planning for and implementing the restarting of defined business operations following an abnormal operating condition, usually beginning with the most critical or time-sensitive functions and continuing along a planned sequence to address all identified areas required by the business.

Contingency planning—The process of developing advance arrangements and procedures that enable a jurisdictional utility to respond to an event that could occur by abnormal operating conditions.

Critical functions—Business activities or information that cannot be interrupted or unavailable for several business days without significantly jeopardizing operations of the organization.

[*Cyber security*—The measures designed to protect computers, software and communications networks that sup-port, operate or otherwise interact with the company's operations.]

[*Cyber security plan*—A written plan that delineates a jurisdictional utility's information technology disaster plan.]

Emergency response plan—A written plan describing the actions a jurisdictional utility will take if an abnormal operating condition exists.

Infrastructure—The systems and assets so vital to the utility that the incapacity or destruction of the systems and assets would have a debilitating impact on security, economic security, public health or safety, or any combination of those matters.

Jurisdictional utility—A **public** utility subject to the reporting requirements of § 27.10, § 29.43, § 31.10, § 33.103, § 57.47, § 59.48, § 61.28, § 63.36 or § 65.19.

Mission critical—A term used to describe essential equipment or facilities to the organization's ability to perform necessary business functions.

Physical security—The physical **[(material)]** measures designed to safeguard personnel, property and information.

Physical security plan—A written plan that delineates the response to security concerns at mission critical equipment or facilities.

Responsible entity—The person or organization within a jurisdictional utility designated as the security or emergency response liaison to the Commission.

[*Self Certification Form*—The Public Utility Security Planning and Readiness Self Certification Form.]

Test—A trial or drill of physical security, **[cyber security,]** emergency response and business continuity plans. **[Testing may be achieved through a sum of continuous partial testing rather than one distinct annual drill when an entire plan is tested from beginning to end.]**

§ 101.3. Plan requirements.

(a) A jurisdictional utility shall develop and maintain written physical **[and cyber]** security, emergency response and business continuity plans.

(1) A physical security plan must, at a minimum, include specific features of a mission critical equipment or facility protection program and company procedures to follow based upon changing threat conditions or situations.

(2) **[A cyber security plan must, at a minimum, include:**

(i) Critical functions requiring automated processing.

(ii) Appropriate backup for application software and data. Appropriate backup may include having a separate distinct storage media for data or a different physical location for application software.

(iii) Alternative methods for meeting critical functional responsibilities in the absence of information technology capabilities.

(iv) A recognition of the critical time period for each information system before the utility could no longer continue to operate.] **{Reserved}.**

(3) A business continuity plan must, at a minimum, include:

(i) Guidance on the system restoration for emergencies, disasters and mobilization.

(ii) Establishment of a comprehensive process addressing business recovery, business resumption and contingency planning.

(4) An emergency response plan must, at a minimum, include:

(i) Identification and assessment of the problem.

(ii) Mitigation of the problem in a coordinated, timely and effective manner.

(iii) Notification of the appropriate emergency services and emergency preparedness support agencies and organizations.

(b) A jurisdictional utility shall review and update these plans annually.

(c) A jurisdictional utility shall maintain and implement an annual testing schedule of these plans. **Testing may be achieved through a sum of continuous partial testing rather than one distinct annual drill when an entire plan is tested from beginning to end.**

(d) **[A jurisdictional utility shall demonstrate compliance with subsections (a)—(c), through submittal of a Self Certification Form which is available at the Secretary's Bureau and on the Commission's website.]** **{Reserved}.**

(e) A plan shall define roles and responsibilities by individual or job function.

(f) The responsible entity shall maintain a document defining the action plans and procedures used in subsection (a).

§ 101.4. **[Reporting requirements.]** **{Reserved}.**

[(a) A utility under the reporting requirements of § 27.10, § 57.47, § 59.48, § 61.28, § 63.36 or § 65.19 shall file the Self Certification Form at the time each Annual Financial Report is filed, under separate cover at Docket No. M-00031717.]

[(b) A utility not subject to the financial reporting requirements in subsection (a), but subject to the reporting requirements of § 29.43, § 31.10 or § 33.103 (relating to assessment reports; assessment reports; and reports) shall file the Self Certification Form at the time each Annual Assessment Report is filed, under separate cover at Docket No. M-00031717.]

§ 101.5. **[Confidentiality of self certification form.]** **{Reserved}.**

[A Self Certification Form filed at the Commission is not a public document or record and is deemed confidential and proprietary.]

§ 101.6. Compliance.

(a) **[The Commission will review a Self Certification Form filed under § 101.4 (relating to reporting requirements).]** **{Reserved.}**

(b) The Commission may review a **jurisdictional** utility's **[cyber security plan,]** physical security plan, emergency response plan and business continuity plan under 66 Pa.C.S. §§ 504—506 (relating to reports by public utility; duty to furnish information to commission; and inspection of facilities and records).

(c) The Commission may inspect a **jurisdictional** utility's facility, to the extent **[utilized] used** for or necessary to the provision of utility service, to assess performance of its compliance monitoring under 66 Pa.C.S. §§ 504—506.

(d) A **jurisdictional** utility that has developed and maintained a **[cyber security,]** physical security, emergency response or business continuity plan under the directive of another state or Federal entity that meets the requirements of § 101.3 (relating to plan requirements) may **[utilize] use** that plan for compliance with this subpart, upon the condition that a Commission representative be permitted to review the **[cyber security,]** physical security, emergency response or business continuity plan. A jurisdictional utility that **[is utilizing] uses** another entity's plan shall briefly describe the alternative plan and identify the authority that requires the alternative plan **[along with the Self Certification Form filed with the Commission].**

§ 101.7. Applicability.

This chapter does not apply to an entity regulated by the Federal Railroad Safety Act (FRSA) (49 U.S.C.A. §§ 20101—20153) and the Hazardous Materials Transportation Act (HMTA) (49 U.S.C.A. §§ 5101—5127) **[, if by August 10, 2005, it submits a certification to the Commission indicating that it has its own written physical and cyber security, emergency response and business continuity plans in place and is in compliance with the FRSA and HMTA].**

CHAPTER 103. CYBERSECURITY EVALUATIONS, PROGRAMS, STANDARDS, AND PLANS

103.1. Purpose

This chapter imposes objective standards, and for certain classes of public utilities specific evaluations, programs and plans, to ensure that each jurisdictional public utility using information technology, operational technology, or supervisory control and data acquisition, or collecting personal information as defined in this chapter, is meeting an appropriate level of cybersecurity fitness.

103.2. Definitions

Air gapped—An interface between two systems at which they are not connected physically, and any logical connection is not automated. Access between systems is done manually and under human control on the premises of the air gapped systems.

Application—A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed.

Asset—Anything that has value to an organization, including, but not limited to any application, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), operational technology (OT), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

Class 1 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility serving 100,000 or more customers.

Class 2 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility serving at least 3,300 customers but less than 100,000 customers.

Class 3 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility serving less than 3,300 customers.

Class 4 utility—Any common carrier that (1) electronically collects and stores personal information; (2) uses IT; or (3) uses OT.

Class 5 utility—Any electric utility, gas utility, steam utility, wastewater utility or water utility that does not (1) electronically collect or store personal information; (2) use IT; and (3) use OT.

Cloud—A ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and

services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Common carrier— Any entity that holds out, offers, or undertakes, directly or indirectly, service for compensation to the public for the transportation of passengers or property, or both, or any class of passengers or property, between points within this Commonwealth by, through, over, above, or under land, water, or air, including forwarders, but not including contract carriers by motor vehicles, or brokers, or any bona fide cooperative association transporting property exclusively for the members of such association on a nonprofit basis. The term does not include a transportation network company or a transportation network company driver.

Confidential security information (CSI)—The term as defined in section 2 of Act 156 (35 P. S. § 2141.2).

Continuity of operations plan (COOP)—A predetermined set of procedures that describe how a public utility's mission-essential functions will be sustained in the event of a cyber or disaster event.

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentications, confidentiality, and nonrepudiation.

Cybersecurity Evaluation Tool (CSET)—A stand-alone desktop application that systematically guides asset owners and operators through evaluating operational and information technology cybersecurity, offered by the Department of Homeland, Cybersecurity and Infrastructure Security Agency (CISA).

Cybersecurity plan—A formal document that provides an overview of the requirements for an organization-wide cybersecurity program and describes the program management controls and common controls in place for meeting those requirements.

Disaster recovery plan (DRP)—The procedures that describe how an organization's Information Technology, Operations Technology, or Cloud Infrastructure will be recovered because of a cyber or disaster event**.**

Electric utility—Any entity that owns or operates in this Commonwealth equipment or facilities for producing, generating, transmitting, distributing, or furnishing electricity for the production of light, heat, or power to or for the public for compensation.

Gas utility—Any entity that owns or operates in this Commonwealth equipment or facilities for producing, generating, transmitting, distributing or furnishing natural or

artificial gas for the production of light, heat, or power to or for the public for compensation.

Governance program—A program that includes the organizational mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements relating to cybersecurity. The governance program comprises governance policies and procedures, risk management strategies, defines oversight responsibilities for the public utility, and identifies individual roles, responsibilities, and authorities.

Incident response program—A program that includes an incident management process and procedure, has an incident identification and analysis process and procedure, establishes a communications policy and procedure, and implements a mitigation protocol.

Information technology (IT)—computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IT components include computers and associated peripheral devices, firmware, computer operating systems, utility/support software, and communications hardware and software.

NIST—The National Institute of Standards and Technology, an agency within the United States Department of Commerce.

NIST Special Publication 800-53—The current version of this NIST catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

NIST Special Publication 800-82—The current version of this NIST guidance on how to secure operational technology (OT) while addressing their unique performance, reliability, and safety requirements.

NIST Cybersecurity Framework (CSF)—The current version of the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Operational technology (OT)—A broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include SCADA, industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

Personal information (PI)—An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

(i) Social Security number.

(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.

(iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(vi) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records or widely distributed media.

Public utility—As defined in 66 Pa.C.S. § 102 (relating to definitions).

Recovery management program—A program that includes a disaster recovery policy and procedure, a resiliency policy and procedure, a continuance of operations policy and procedure, and includes cybersecurity training and yearly tabletop exercises.

Risk assessment—The process of identifying cybersecurity risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system; incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

Risk mitigation plan—A plan that prioritizes, evaluates, and implements the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Security management program—A program that addresses identity management, authentication, and access controls, data security, platform security, technology infrastructure resilience and physical security controls. A security management program must ensure that:

(i) IT, OT, and cloud environment architectural reviews are completed prior to implementation to ensure they comply with the utility’s governance policies and procedures.

(ii) Application development best practices are reviewed and enforced and all in-house applications and procured applications are reviewed for security vulnerabilities prior to being placed into production.

(iii) Changes to system configurations and patch management processes and procedures are documented and system operators are made aware of these changes.

(iv) All confidential data is encrypted at rest and in transit.

(v) All network traffic is documented, and proper security mechanisms are in place to protect the internal and external networks.

(vi) All physical access controls are documented and monitored and comply with applicable standards.

(vii) All IT, OT, cloud, and physical access contracts with any third party are reviewed for compliance with applicable standards and to ensure that all potential vulnerabilities are identified and addressed as part of the contractual agreements and licenses.

Steam utility— As defined in 52 Pa.C.S. § 61.1 (relating to definitions).

Supervisory control and data acquisition (SCADA)— A computerized system that is capable of gathering and processing data and applying operational controls over long distances.

Telecommunications utility—Any entity that owns or operates in this Commonwealth equipment or facilities for conveying or transmitting messages or communications by telephone or telegraph or domestic public land mobile radio service including, but not limited to, point-to-point microwave radio service for the public for compensation. The term does not include any person or corporation, not otherwise a public utility, who or which furnishes mobile domestic cellular radio telecommunications service.

Third Party–An entity that is external to a public utility, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums and investors, with or without a contractual relationship to the public utility.

Threat management program—A program that provides threat identification, threat monitoring, and threat detection and threat isolation capabilities. A threat management program must utilize tools that can discover anomalies, search for indicators of compromise, and detect unauthorized activities and events that can lead to cybersecurity incidents.

Vulnerability assessment–A systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide

data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability management program—A program that identifies the public utility's assets that enable it to achieve its business purposes which are identified and managed consistently along with their relative importance to the public utility's objectives and risk strategy. A vulnerability management program must include: an asset management inventory; vulnerability and risk assessments; risk mitigation plans; and improvement process and procedures.

Water utility—Any entity that owns or operates in this Commonwealth equipment or facilities for diverting, developing, pumping, impounding, distributing, or furnishing water to or for the public for compensation.

Wastewater utility—Any entity that owns or operates in this Commonwealth equipment or facilities for wastewater collection, treatment, or disposal for the public for compensation.

103.3. Cybersecurity Evaluations and Programs

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

(1) An annual cybersecurity evaluation which:

(i) includes all assets used to provide public utility service in Pennsylvania; and

(ii) uses the CSET, selecting, at a minimum, these assessments and standards:

(A) NIST CSF,

(B) NIST Special Publication 800-53, and

(C) NIST Special Publication 800-82.

(2) A governance program.

(3) A security management program.

(4) A vulnerability management program.

(5) A risk management program.

(6) A threat management program.

(7) An incident response program.

(8) A recovery management program.

(b) A Class 2 utility shall maintain and adhere to the following:

(1) An annual cybersecurity evaluation which:

(i) includes all assets used to provide public utility service in Pennsylvania; and

(ii) uses the CSET to conduct a NIST CSF assessment.

(2) A governance program.

(3) A security management.

(4) A vulnerability management program.

(5) A risk management program.

(6) A threat management program.

(7) An incident response program.

(8) A recovery management program.

(c) A Class 3 utility and a Class 4 utility shall maintain and adhere to the following:

(1) An annual cybersecurity evaluation which:

(i) includes all assets used to provide public utility service in Pennsylvania; and

(ii) uses the CSET to conduct a NIST CSF assessment.

(2) A cybersecurity plan that is updated annually to address the findings of the annual NIST CSF assessment.

(3) An annual vulnerability assessment.

(4) A risk mitigation plan that is updated annually to address the risks identified by the vulnerability assessment.

(5) An incident response plan that is formally approved by executive management, identifies key personnel, clarifies their roles and responsibilities, and provides guidance on key activities needed to restore systems back to the state before the incident happened.

(6) A COOP.

(7) a disaster recovery plan.

(d) a telecommunications utility shall develop, maintain, and adhere to a written cybersecurity plan, which must, at a minimum, include:

(1) Critical functions requiring automated processing.

(2) Appropriate backup for application software and data. Appropriate backup may include having a separate distinct storage media for data or a different physical location for application software.

(3) Alternative methods for meeting critical functional responsibilities in the absence of information technology capabilities.

(4) A recognition of the critical time period for each information system before the telecommunications utility could no longer continue to operate.

(e) a Class 5 utility is not subject to the requirements of this Section.

103.4. Annual Certification.

(a) A Class 1 utility shall file with the Commission on an annual basis a certification that the utility complies with the requirements of 52 Pa. Code § 103.3(a).

(b) A Class 2 utility shall file with the Commission on an annual basis a certification that the utility complies with the requirements of 52 Pa. Code § 103.3(b).

(c) A Class 3 utility and a class 4 utility shall file with the Commission on an annual basis a certification that the utility complies with the requirements of 52 Pa. Code § 103.3(c).

(d) A Class 5 utility shall file with the Commission on an annual basis a certification that it (1) does not electronically collect or store PI; (2) does not use IT; and (3) does not use OT, or only operates OT in an air gapped environment.

(e) A telecommunications utility shall file with the Commission on an annual basis a certification that that:

(i) the telecommunications utility maintains and conforms to a cybersecurity plan that complies with the requirements of 52 Pa. Code § 103.3(d).

(ii) that the telecommunications utility's cybersecurity plan been reviewed and updated in the past year.

(iii) that the telecommunications utility's cybersecurity plan is tested annually.

(iv) the telecommunications utility performed a vulnerability or risk assessment analysis for cybersecurity in the past year.

(f) A public utility under the reporting requirements of § 27.10, § 57.47, § 59.48, § 61.28, § 63.36 or § 65.19 shall file its certification at the time each Annual Financial Report is

filed with the Commission. A utility not subject to such financial reporting requirements, but subject to the reporting requirements of § 29.43, § 31.10 or § 33.103 (relating to assessment reports; assessment reports; and reports) shall file an annual certification with the Commission at the time each Annual Assessment Report is filed. A wastewater utility shall file its certification by April 30 each year.

(g) An annual certification filed at the Commission is not a public document or record and is deemed CSI.

103.5. Waiver.

(a) A public utility may petition the Commission for a waiver from any of the cybersecurity evaluation or program standards set forth in section 103.3(a), (b) or (c) of this Chapter. The Commission may grant the petition if the public utility has demonstrated that notwithstanding the requested exemption, it will maintain and comply with cybersecurity programs, plans, and standards that provide a reasonable level of cybersecurity fitness relative to its Pennsylvania assets and customers using state of the art cybersecurity equipment, methods, and software.

(b) If the Commission grants a public utility's petition for waiver consistent with subsection (a), the public utility shall file with the Commission on an annual basis an appropriate certification that the public utility maintains and conforms to its exempted cybersecurity program.

103.6. Procedure When External References Are Updated.

(a) If any cybersecurity application, publication, standard or requirement published or promulgated by an entity other than the Commission and incorporated by reference into this Chapter is updated by the relevant entity, the Commission will publish notice of the effective date in Pennsylvania of said update in the *Pennsylvania Bulletin*.

(b) Notwithstanding paragraph (a), an update under paragraph (a) shall take effect 120 days after the effective date of the update as determined by the relevant entity unless the Commission publishes a notice in the *Pennsylvania Bulletin* stating that the amendment or modification may not take effect.

(c) A Commission notice issued under paragraph (b) will provide an opportunity for public comment on the update, including whether it is advisable for the update to take effect as referenced in this Chapter. The Commission notice will identify the period during which comments may be filed with the Commission following publication of the notice in the *Pennsylvania Bulletin*.

(d) An update under paragraph (a) that is the subject of a Commission notice pursuant to paragraph (c) may become effective by further action of the Commission upon its review of the cybersecurity application, publication, standard or requirement published or promulgated and any comments filed pursuant to notice in the *Pennsylvania Bulletin*.

103.7. Compliance.

(a) The Commission will review an annual certification form filed under § 103.3 (relating to annual certification).

(b) The Commission may review a public utility's cybersecurity evaluations, programs, assessments and plans under 66 Pa.C.S. §§ 504—506 (relating to reports by public utility; duty to furnish information to commission; and inspection of facilities and records).

(c) The Commission may inspect a public utility's assets, to the extent used for or necessary to the provision of utility service, to assess performance of its cybersecurity programs plans under 66 Pa.C.S. §§ 504—506.

CHAPTER 104. CYBERSECURITY INCIDENT REPORTING

104.1. Definitions

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.

Exfiltration—The unauthorized transfer of information from an information system.

Information Technology (IT)— computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IT components include computers and associated peripheral devices, firmware, computer operating systems, utility/support software, and communications hardware and software.

Operational Technology (OT)—A broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

Pennsylvania State Police Criminal Intelligence Center (PaCIC)— Pennsylvania's coordination center for the federal, local, and private sector partners necessary to prevent, protect against, mitigate the effects of, respond to, and recover from emergencies and disasters.

Personal information (PI)—An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

(i) Social Security number.

(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.

(iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(vi) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records or widely distributed media.

Public utility—As defined in 66 Pa.C.S. § 102 (relating to definitions). The term does not include subsection (1)(vi) of the definition of "public utility" (relating to telecommunications utilities)

Public Utility Code—Title 66 of the Pennsylvania Consolidated Statutes (relating to public utilities).

Ransomware—A type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.

Third Party–An entity that is external to a public utility, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums and investors, with or without a contractual relationship to the public utility.

104.2. Reporting Requirements

(a) A public utility shall report to the Commission any cyber incident that arises on the network of a public utility or the network of a third-party connected to, or relied upon by, a public utility, which causes in whole or in substantial part any of the following:

(i) a service outage.

(ii) a compromise or damage to, or loss of control of, IT or OT used to provide public utility service in Pennsylvania.

(iii) exfiltration of PI of Pennsylvania residents.

(iv) 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.

(v) a situation which endangers the health, safety or welfare of the public utility's customers, employees, or the public at large.

(b) A public utility shall report a cyber incident that meets one or more of the criteria in subsection (a) of this Section within 72 hours after the public utility determines that a

cyber incident occurred. The Commission will maintain telephone lines for this purpose and will notify each utility of the numbers to be called. The public utility shall make its report by contacting a Commission-designated representative by telephone and verbally providing the following information:

(i) Public utility name.

(ii) Public utility point of contact.

(iii) Synopsis of the cyber incident.

(iv) Whether the cyber incident impacts the public utility's information systems or operational technology.

(v) Whether there is any risk that the cyber incident is capable of moving laterally to any additional information system or operational technology.

(vi) Whether the cyber incident is causing a service outage, and if so, how many customers are impacted, how large of an area/region is impacted, and what is the estimated time for services to be recovered.

(vii) Whether personal information has been exfiltrated.

(viii) Whether the public utility contacted any outside entities about the incident.

(ix) Whether the utility would like the PUC to inquire about assistance from state partners.

(c) A public utility shall report to the Commission a cyber incident that involves ransomware and meets one or more of the criteria in subsection (a) of this Section within 24 hours after the public utility determines that a ransomware incident occurred. The Commission will maintain telephone lines for this purpose and will notify each utility of the numbers to be called. The public utility shall make its report by contacting a Commission-designated representative by telephone and verbally providing, in addition to the information listed in subsection (b)(i)-(ix) of this Section, the following information:

(i) The amount, if any, that was paid to the ransomware actor.

(ii) Whether any payment made resulted in restoration of access to and control over the encrypted information.

(iii) Measures the utility intends to implement to ensure that it will not continue to be extorted by the ransomware actor.

(d) A public utility may use a cybersecurity incident report that it has submitted to satisfy the reporting requirements of a separate state or federal agency so long as such report provides the information required in subsections (a)-(c).

(e) A public utility shall report a cyber incident that meets one or more of the criteria in subsection (a) of this Section to the PaCIC within 24 hours.