PENNSYLVANIA
PUBLIC UTILITY COMMISSION
Harrisburg PA 17105-3265

Public Meeting held April 24, 2025

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	L-2022-3034353

SUPPLEMENTAL ADVANCE NOTICE OF PROPOSED RULEMAKING ORDER

BY THE COMMISSION:

The Pennsylvania Public Utility Commission (PUC) enters this Supplemental Advance Notice of Proposed Rulemaking Order (Supplemental ANOPR or Order) to review its current regulations relating to cybersecurity.[1] At its November 10, 2022 Public Meeting, the PUC adopted an Advance Notice of Proposed Rulemaking in Docket No. L-2022-3034353, *Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting* (Entered Nov. 10, 2022) (November 2022 ANOPR).

[1] The Commission's existing regulations use "cyber security" in lieu of the widely accepted "cybersecurity." For purposes of this Order, "cybersecurity" shall be used, except when quoting directly from the existing regulations.

The PUC entered the November 2022 ANOPR to review its current regulations relating to cybersecurity. These regulations fall into two groups: (1) cyber attack[2] reporting regulations and (2) self-certification regulations (collectively, "existing regulations").

Cyber attack reporting regulations include:

- 52 Pa. Code §§ 57.11 (relating to accidents) for electricity public utilities,
- 59.11 (relating to accidents) for gas public utilities,
- 61.11 (relating to accidents) for steam utilities,
- 65.2 (relating to accidents) for water public utilities.

Self-certification regulations include:

- 52 Pa. Code §§ 101.1–101.7 (Chapter 101, relating to public utility preparedness through self-certification) for jurisdictional utilities,
- 61.45 (relating to security planning and emergency contact list) for steam utilities.

In the November 2022 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 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. The November 2022 ANOPR requested that comments be organized around 15 numbered topics, which were listed both in the main body of the November 2022 ANOPR and in a separate Appendix A (Topics for Comment). These topics were:

[2] The Commission's prior orders use "cyber attack" whereas its existing regulations use "cyber-attack." For purposes of this Supplemental ANOPR, "cyber attack" will be used, except when quoting directly from the existing regulations.

- 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.

The November 2022 ANOPR was published in the Pennsylvania Bulletin at 52 Pa.B. 7507 (December 10, 2022). Comments were due to be filed with the PUC no later than February 8, 2023.

Nineteen (19) comments[3] were timely filed in response to the November 2022 ANOPR:

- Comments of AT&T Corp., Teleport Communications America, LLC and SBC Long Distance, LLC (AT&T),
- Comments of The Broadband Communications Association of Pennsylvania (BCAP),
- Comments of Citizens' Electric Company of Lewisburg, Pa., Wellsboro Electric Company and Valley Energy, Inc. (C&T Utilities),
- Comments of Columbia Gas of Pennsylvania, Inc. (Columbia Gas),
- Comments of Duquesne Light Company (Duquesne Light),
- Comments of Energy Association of Pennsylvania (EAP),
- Comments of FirstEnergy,

[3] On February 8, 2023, the Pennsylvania Office of Small Business Advocate filed a letter in Docket No. L-2022-3034353 advising that it would not be filing comments and Aqua Pennsylvania, Inc. filed a letter in the same docket indicating that its joint comments with Peoples Natural Gas Company LLC would be filed by Peoples.

- Comments of NRG Energy, Inc. (NRG),
- Comments of Office of Consumer Advocate (OCA),
- Comments of Pennsylvania-American Water Company (PAWC),
- Comments of Pennsylvania Chamber of Business and Industry (PA Chamber),
- Comments of Pennsylvania Telephone Association (PTA),
- Comments of PPL Electric Utilities Corporation (PPL Electric),
- Comments of PECO Energy Company (PECO),
- Comments of Retail Energy Supply Association (RESA),
- Comments of United States Environmental Protection Agency Region III (EPA Region III),
- Comments of 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. (Verizon),
- Joint Comments of Aqua Pennsylvania, Inc. and Peoples Natural Gas Company LLC (Aqua/Peoples),
- Joint Comments of Community Utilities of Pennsylvania Inc. and Columbia Water Company (CUPA/CWC),
- Joint Comments of Tri-Co Connections, LLC and Claverack Communications, LLC (TCC/CC).

The Commission greatly appreciates each of these thoughtful and detailed comments. This Order will not attempt to summarize all the comments the Commission previously received but will refer to selected comments as appropriate to inform and illustrate the topics discussed herein.

In this Order, the Commission notes several significant events in cybersecurity and requests additional comments on limited, specified topics. First, a growing chorus of state and federal authorities have highlighted the importance of sector specific agencies increasing the intensity of their oversight into the cybersecurity fitness of their regulated entities, including adherence to defined standards. Second, the United States Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA) released its notice of proposed rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)[4] last year, and identified that the purpose of its forthcoming incident reporting regulations will be to inform CISA's active, real-time role in incident detection, response and recovery across a diverse array of critical infrastructure industries.[5]

The Commission seeks comments from interested stakeholders, including members of the regulated industry, statutory advocates, the public, and any other interested parties about whether the existing regulations are sufficient or if they need to be revised to ensure that they address public utility fitness in the current and anticipated future cybersecurity threat landscapes. Throughout this Supplemental ANOPR, as with the November 2022 ANOPR, any proposed changes, consolidations, deletions, and additions to the existing regulations shall be referred to as "revisions." Commenters are directed to address their comments to the list of questions set forth in Appendix A to this Supplemental ANOPR. The Commission notes that these questions are different from the ones listed in the initial November 2022 ANOPR. To ensure comments are fully considered, commenters should identify which question(s) their comments address, noting that there is a "catch all" question to account for comments which may be relevant to the discussion but do not fit neatly in any of the specific questions.

[4] DHS CISA, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Federal Register Vol. 89, No. 66 at 23644 (Apr. 4, 2024).
[5] CISA Notice of Proposed Rulemaking, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Federal Register Vol. 89, No. 66 at 23644 (Apr. 4, 2024).

BACKGROUND

Regulating Cybersecurity Standards

National Cybersecurity Strategy (March 2023)

In March 2023, the Biden Administration released the National Cybersecurity Strategy, providing a cohesive national framework for enhancing cybersecurity across all critical infrastructure sectors.[6] Therein, the Administration encouraged states to use their existing regulatory authority to set cybersecurity requirements in a deliberate and coordinated manner.[7] The Biden Administration also counseled regulatory agencies to minimize the cost and burden of compliance with cybersecurity standards, including minimizing conflict and duplication between regulatory regimes.[8] The Administration also highlighted that Federal response to cyber incidents must be coordinated and tightly integrated with state partners.[9]

NARUC Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources (February 2024)

The National Association of Regulatory Utility Commissioners (NARUC) issued a set of cybersecurity baselines in February 2024, focusing specifically on electric distribution systems and distributed energy resources (DER).[10] These baselines were developed in consultation with stakeholders across the energy industry, federal agencies, and cybersecurity experts, and were designed to establish foundational cybersecurity

[6] White House, National Cybersecurity Strategy (March 2023) at 3, formerly available online at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (last accessed November 15, 2024). As of April 14, 2025, the foregoing link is not available online. The same is true for some (but not all) of the other federal government documents referenced herein that were released during the Biden administration. Whether this lack of availability reflects a change in cybersecurity policy by the Trump administration is not clear at this time.
[7] *Id*. at 8.
[8] *Id*. at 9.
[9] *Id*. at 7.
[10] NARUC, Cybersecurity Baselines for Electric Distribution Systems and DER (February 2024) at 2, available online at https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/ (last accessed April 14, 2025).

measures for electric distribution utilities and DER providers and aggregators.[11] The baselines represent an application of CISA's Cybersecurity Performance Goals (CPGs) to the electric distribution system context.[12] The baselines identify standard practices such as regular vulnerability assessments (including supply chains), network segmentation, comprehensive incident response plans and a focus on securing operational technology (OT) to mitigate the growing cyber risks facing the electric distribution sector.[13]

White House Letter to Governors on Water & Wastewater Systems (March 2024)

On March 18, 2024, the White House issued a letter to the governors of each state, including Governor Shapiro, noting recent cyberattacks by foreign state threat actors against United States water and wastewater systems.[14] The letter notes that drinking water and wastewater systems are an attractive target for cyberattacks because they are a lifeline sector but often lack the resources to adopt rigorous cybersecurity practices.[15] The letter asks states for assistance in addressing the pervasive risk of cyberattacks on drinking water systems and to ensure that all water systems comprehensively assess their current cybersecurity practices to identify any significant vulnerabilities, deploy practices and controls to reduce cybersecurity risks, and develop plans to prepare for, respond to, and recover from a cyber incident.[16]

[11] *Id*. at 3.
[12] *Id*. at 4.
[13] *Id*. at 4-11.
[14] Letter from Michael S. Regan, Administrator, U.S. Environmental Protection Agency, and Jake Sullivan, Assistant to the President for National Security Affairs to Governors (March 18, 2024) at 1, available online at https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf (last accessed April 14, 2025).
[15] *Id*.
[16] *Id*. at 1-2.

National Security Memorandum on Critical Infrastructure Security and Resilience (April 2024)

The federal government issued a National Security Memorandum in April, 2024 (NSM-22) to strengthen cybersecurity and resilience across U.S. critical infrastructure.[17] NSM-22 recognizes that safeguarding critical infrastructure is a responsibility shared by Federal agencies, state, local, tribal, and territorial entities as well as the public or private owners and operators of critical infrastructure.[18] NSM-22 calls upon sector-specific agencies, including State regulatory entities, to establish and implement minimum requirements for risk management, leveraging existing guidance where applicable.[19] NSM-22 counsels that regulatory frameworks should be risk- and performance-based when feasible; informed by existing requirements, standards, and guidelines; aligned to reduce unnecessary duplication; complementary to voluntary public-private collaboration; and scalable and adaptable to an evolving risk environment.[20]

DHS Memorandum on Strategic Guidance for U.S. Critical Infrastructure (June 2024)

In June 2024, DHS issued a memorandum titled "Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience."[21] The DHS Memorandum recognizes that energy grids, water and wastewater systems, transportation networks, healthcare facilities, communication networks, and other essential systems are vital for public safety, economic security, and national security but the increasing interconnectivity of critical infrastructure systems and reliance upon global technologies

[17] White House, *National Security Memorandum on Critical Infrastructure Security and Resilience/NSM-22* (April 30, 2024), formerly available online at https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (last accessed November 15, 2024). As of April 14, 2025, the foregoing link is not available online.
[18] *Id*. at ¶ 1.
[19] *Id*. at ¶ 3.
[20] *Id*.
[21] Department of Homeland Security, Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024-2025) (June 14, 2024) (DHS Memorandum), available online at https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-critical-infrastructure-security-resilience.pdf (last accessed April 14, 2025).

and supply chains make these systems susceptible to a myriad of threats.[22] The DHS Memorandum states that sector-specific agencies should encourage critical infrastructure owners and operators and, where applicable, hold them accountable for implementing baseline controls that improve their security and resilience to cyber and all hazard threats.[23] The DHS Memorandum identifies the CISA CPGs and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 as existing tools that provide a common set of protections against threats, such as ransomware.[24] DHS pledged to work with regulators and private sector entities to ensure that baseline requirements are risk-informed, performance-based, and to the extent feasible, harmonized and to develop tools that support the adoption of such requirements.[25]

Cybersecurity Incident Reporting

CISA Cyber Incident Reporting NOPR (April 2024)

CIRCIA provides for critical infrastructure operators to report covered cybersecurity incidents to CISA.[26] In April 2024, CISA issued a Notice of Proposed Rulemaking (NOPR) to implement CIRCIA.[27] CISA notes that CIRCIA requires covered entities to report covered cyber incidents within 72 hours after the entity reasonably believes that the incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made.[28] CISA states that CIRCIA will enhance its ability to identify trends and track cyber threat activity across the cyber threat landscape[29] and develop a comprehensive and coordinated

[22] *Id*. at 1.
[23] *Id*. at 4.
[24] *Id*.
[25] *Id.*
[26] 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*.).
[27] DHS CISA, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Federal Register Vol. 89, No. 66 at 23644 (Apr. 4, 2024).
[28] *Id.* at 23648; *and see* 6 U.S.C. § 681b(a).
[29] *Id.*

approach to understanding cyber incidents across critical infrastructure sectors, enabling a coordinated, informed U.S. response to the foreign governments and criminal organizations conducting cyberattacks against the U.S.[30]

CISA identified two main themes in its regulatory objectives. First, to achieve the multiple goals of its proposed regulations, including identifying adversary tactics, techniques and procedures (TTPs) and providing early warnings of cyber threats across critical infrastructure sectors, CISA determined that it needs to receive a large quantity of cyber incident reports from across the spectrum of critical infrastructure, supported by systematic collection of cyber incident information reliably and at scale.[31] Second, CISA identified the importance of timeliness in both the receipt of reports and CISA's ability to analyze and share information gleaned from those reports, to enable early visibility and increase the likelihood that the critical infrastructure community may address identified vulnerabilities and secure themselves against the latest adversary TTPs.[32]

DISCUSSION

The Commission appreciates the detailed and thoughtful comments submitted in response to its November 2022 ANOPR. However, the unrelenting pace of events in cybersecurity requires a partial refresh, focusing on specific topics.

Ongoing Threats to Critical Infrastructure

Since the November 2022 ANOPR, the threat level for critical infrastructure remains very high. The former United States Director of National Intelligence assesses that "China remains the most active and persistent cyber threat to… critical infrastructure

[30] *Id.* at 23649.
[31] *Id*. at 23652.
[32] *Id*. at 23653.

networks,"[33] "Russia maintains its ability to target critical infrastructure"[34] and "[t]ransnational organized criminals involved in ransomware operations are improving their attacks, extorting funds, disrupting critical services, and exposing sensitive data," including critical infrastructure.[35] DHS assesses that "domestic and foreign adversaries almost certainly will continue to threaten the integrity of US critical infrastructure, in part, because they perceive targeting these sectors would have cascading impacts on US industries and our standard of living."[36] DHS further assesses that "[People's Republic of China] state-sponsored cyber actors have pre-positioned cyber exploitation and attack capabilities for disruptive or destructive cyber attacks against US critical infrastructure in the event of a major crisis or conflict with the United States" and "[t]hese compromises have been primarily lifeline sectors, including the communications, energy, transportation, and water and wastewater sectors."[37]

These assessments have been borne out by recent cyber incidents involving critical infrastructure. Beginning in November, 2023, the Iranian Islamic Revolutionary Guard Corps (IRGC) accessed multiple US-based water and wastewater systems, including the Municipal Water Authority of Aliquippa, that operated a specific brand of programmable logic controllers that ship with a default password.[38] IRGC hackers compromised the default credentials and defaced the controller's user interface, thereby "prevent[ing] the compromised devices from operating as intended."[39] According to news reports

---

[33] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, at 11 (Feb. 5, 2024), available online at: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (last accessed April 14, 2025).
[34] *Id*. at 16.
[35] *Id*. at 37.
[36] Department of Homeland Security, *Homeland Threat Assessment 2025*, at 21 (September 2024), available online at: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (last accessed April 14, 2025).
[37] *Id*. at 22.
[38] CISA Cybersecurity Advisory, IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (Dec. 18, 2024), available online at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a (last accessed April 14, 2025).
[39] *Id.*

following the incident, "[c]ustomers weren't affected because crews alerted by an alarm quickly switched to manual operation — but not every water authority has a built-in manual backup system."[40]

In October, 2024, hackers sponsored by the PRC "infiltrated United States telecommunications companies (including internet service providers)," in what authorities refer to as "Salt Typhoon."[41] News outlets reported that "hackers may have targeted the systems used to provide court-approved access to communication systems used for investigations by law enforcement and intelligence agencies."[42] The Salt Typhoon hackers "may have sought access to these systems and companies to gain access to presidential candidate communications" with which "they could potentially retrieve unencrypted communication (e.g., voice calls and text messages)."[43] Salt Typhoon is simply the latest in a string of PRC-sponsored hacking enterprises that have targeted U.S. critical infrastructure, including Volt Typhoon (which uses "built-in tools on the target network to execute objectives without installing malware") and Flax Typhoon (which "compromised hundreds of internet-of-things (IOT) devices to create a botnet that they used to carry out attacks.").[44]

Moving Towards Defined Cybersecurity Standards

As detailed above, 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. The

[40] AP, States and Congress wrestle with cybersecurity after Iran attacks small town water utilities (January 2, 2024), available online at https://apnews.com/article/water-utilities-hackers-cybersecurity-1c475f5d2ef3b5d52410c93bdeab3aad (last accessed April 14, 2025).
[41] Congressional Research Service, Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications (Nov. 15, 2024), available online at: https://crsreports.congress.gov/product/pdf/IF/IF12798 (last accessed April 14, 2025).
[42] *Id*.
[43] *Id.*
[44] *Id.*

Commission's current Chapter 101 regulations were promulgated in 2005[45] and have not been refreshed to reflect state-of-the-art cybersecurity concepts and standards. At the same time, there are significant gaps in the cybersecurity standards regimes maintained by federal sector specific agencies. For example, the United States Federal Energy Regulatory Commission (FERC) implemented cybersecurity reliability standards, but these only applied to the bulk power system, not local distribution networks.[46]

The United States Environmental Protection Agency (EPA), as the federal sector risk management agency for water, issued a memorandum to state drinking water administrators in March, 2023, "[c]larifying that cybersecurity must be evaluated [by states] in reviewing operational technology that is part of a [public water system's] equipment or operation during sanitary surveys or other state programs[.]"[47] EPA's safe drinking water regulations require "primacy" states[48] to conduct sanitary surveys of their public water systems,[49] and in its memorandum, EPA interpreted primacy states'

---

[45] Revised Final Rulemaking Order, *Rulemaking re Public Utility Security Planning and Readiness*, Pa. PUC Docket No. L-00040166 (entered Mar. 10, 2005) at 1, 35 Pa.B. 24 (June 11, 2005) (Chapter 101 Order).

[46] *See* 6 U.S.C. § 824o(a)(1) ("The term "bulk-power system" means--(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy."); *and see* 16 U.S.C. § 824o(b)(1) ("The Commission shall have jurisdiction, within the United States, over… all users, owners and operators of the bulk-power system… for purposes of approving reliability standards established under this section and enforcing compliance with this section. All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section.").

[47] Memorandum, Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process, U.S.E.P.A., at 2 (Mar. 3, 2023), available online at https://nepis.epa.gov/Exe/ZyNET.exe/P101D7KB.txt?ZyActionD=ZyDocument&Client=EPA&Index=2016%20Thru%202020&Docs=&Query=&Time=&EndTime=&SearchMethod=1&TocRestrict=n&Toc=&TocEntry=&QField=&QFieldYear=&QFieldMonth=&QFieldDay=&UseQField=&IntQFieldOp=0&ExtQFieldOp=0&XmlQuery=&File=D%3A%5CZYFILES%5CINDEX%20DATA%5C16THRU20%5CTXT%5C00000052%5CP101D7KB.txt&User=ANONYMOUS&Password=anonymous&SortMethod=h%7C-&MaximumDocuments=1&FuzzyDegree=0&ImageQuality=r75g8/r75g8/x150y150g16/i425&Display=hpfr&DefSeekPage=&SearchBack=ZyActionL&Back=ZyActionS&BackDesc=Results%20page&MaximumPages=1&ZyEntry=2 (last accessed April 14, 2025).

[48] A "primacy" state is one which applied for and received EPA approval to have primary responsibility for administration and enforcement of primary drinking water regulations and related requirements applicable to public water systems within a State. 40 C.F.R. § 142.2. Pennsylvania is a primacy state.

[49] 40 C.F.R. § 142.10(b)(2).

obligation to examine "[s]ystem management and operation" in its surveys[50] to encompass an evaluation of the system's operational technology cybersecurity.[51] However, EPA was forced to withdraw this memorandum in the face of legal challenges and a stay issued by the U.S. Court of Appeals for the Eight Circuit.[52] In withdrawing the memorandum, EPA encouraged states to voluntarily review public water system cybersecurity programs, either in sanitary surveys, or in "an alternate process" to ensure deficiencies are corrected and public health impacts are minimized.[53]

Conversely, the United States Transportation Security Agency (TSA) is currently proposing comprehensive cybersecurity risk management (CRM) program requirements that would apply to certain large freight railroad, passenger railroad, hazardous liquid and natural gas pipeline utilities, to include those that provide "natural gas distribution or local distribution company (LDC)" services to 275,000 or more meters (or service points)."[54] Indeed, TSA has imposed some measure of cybersecurity program requirements on railroad and pipeline utilities since 2002.[55] Thus it appears that TSA has staked out a federal role in the oversight of the cybersecurity fitness of at least some Commission-jurisdictional utilities operating in the transportation and natural gas sectors.

Commenters to the November 2022 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

[50] 40 C.F.R. § 142.16(b)(3)(i)(G).
[51] U.S.E.P.A. Memorandum at 2.
[52] Joint Stipulation of Dismissal, *American Water Works Association, et al. v. U.S.E.P.A., et al.*, U.S.C.A. (8th Cir.) Docket No. 23-1787 (Oct. 25, 2023).
[53] Memorandum, Withdrawal of Cybersecurity Memorandum of March 3, 2024, U.S.E.P.A. (Oct. 11, 2023), available online at https://www.epa.gov/system/files/documents/2023-10/action-memo_rescinding-cyber-memo_october-2023.pdf (last accessed April 14, 2025).
[54] Notice of Proposed Rulemaking, Enhancing Surface Cyber Risk Management, U.S. Department of Homeland Security, Transportation Security Administration (Nov. 7, 2024), Federal Register, Vol. 89, at 88,508-11.
[55] *Id*. at 88,498-99.

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."[56] 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."[57] 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."[58] However, given the increasing importance of ensuring that our jurisdictional public utilities are adhering to high standards of cybersecurity fitness, and the evident gaps in federal coverage of at least some of the sectors we regulate, regulations requiring adherence to defined standards may be advisable. At the same time, imposing prescriptive regulations on sectors for which federal authorities have already enacted adequate safeguards and requirements may not be in the public interest.

Harmonizing Commission Incident Reporting Regulations with CISA/CIRCIA

In response to the November 2022 ANOPR, commenters expressed a range of views on CISA's ongoing rulemaking to implement CIRCIA. For example, BCAP counseled that "the Commission should forego adoption of new cyber reporting rules pending completion of the CIRCIA implementation proceeding."[59] In BCAP's view, the

[56] Comments of PECO, Pa. PUC Docket No. L-2022-3034353, at 4 (Feb. 8, 2023).
[57] *Id.*
[58] Joint Comments of Community Utilities of Pennsylvania, Inc. and Columbia Water Company, Pa. PUC Docket No. L-2022-3034353, at 2 (Feb. 8, 2023).
[59] Comments of BCAP, at 12.

CIRCIA rulemaking will help the Commission "strik[e] the appropriate balance between ensuring that the government has timely and accurate information about substantial cyber incidents while avoiding over-reporting of incursions that have little or no disruptive effects on the public."[60] BCAP further noted that "deferring action on incident reporting also aligns with the ANOPR's appropriate concern with avoiding duplicative or overlapping regulation."[61] For its part, PAWC recommends that "the Commission should strive to adopt reporting requirements that align with the federal reporting requirements within CIRCIA applicable to utilities"[62] and "[c]onsistent with CIRCIA, utilities should be required to report all 'cyber incidents' that occur to the Commission as well."[63] PAWC further recommends defining "cyber incident" to align with CISA's definition in its regulations implementing CIRCIA, and to adopt CIRCIA's 72-hour time frame for reporting cyber incidents.[64] Finally, FirstEnergy admonished that "the PaPUC not to 'pile on' to what is already covered by CIRCIA or duplicate those efforts in any way."[65]

The Commission agrees with commenters who assert that CISA's rulemaking to implement CIRCIA will reveal important insights and that the Commission should strive to align its reporting requirements, as appropriate with CISA. However, the Commission notes two potential limitations to alignment. One is that CIRCIA does not provide, nor propose, that incident reports be shared with state agencies like the Commission. Thus, the mere fact that utilities will be required to submit CIRCIA incident reports to CISA appears to have no practical benefit to the Commission nor assist the Commission's statutory mission to ensure adequate, safe and reliable public utility service in Pennsylvania.[66] Second, CISA's goals in collecting incident reports are markedly

[60] *Id.*
[61] *Id.*
[62] Comments of Pennsylvania-American Water Company, Pa. PUC Docket No. L-2022-3034353, at 6 (Feb. 8, 2023).
[63] *Id.* at 6-7.
[64] *Id.* at 7.
[65] Comments of FirstEnergy, Pa. PUC Docket No. L-2022-3034353, at 20 (Feb. 8, 2023).
[66] *See* 66 Pa. C.S. § 1501.

different from the Commission's goals (at least as articulated previously). 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.[67] By contrast, the Commission's incident reporting regulations, as articulated so far, are limited to keeping the Commission abreast of service-affecting impacts for continuity of operations and continuity of government (COOP/COG) purposes, and ensuring continuous public utility service to Pennsylvania residents and businesses.[68] Although we do not foreclose recasting our role going forward, to date the Commission has not engaged in threat analysis, information sharing or assisting public utilities with incident response. Thus, it may not be necessary or desirable for the Commission to receive the relatively large volume of incident reports CISA is contemplating.

Staff Working Proposals

Several commenters to the November 2022 ANOPR noted that it was difficult to answer some of the questions posed therein with specificity due to the lack of a concrete proposal. For example, FirstEnergy commented that "[i]t is difficult… to comment on the impacts the changes would have to physical security, emergency response and/or business continuity aspects of the rule or Chapter 101 without seeing the proposed changes."[69] Relative to cost-benefit analysis of new or modified regulations, Duquesne Light commented that it "cannot assess cost-benefit impacts prior to reviewing specific proposed regulatory changes."[70]

---

[67] 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.").
[68] *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).
[69] FirstEnergy Comments at 14.
[70] Comments of Duquesne Light Company, Pa. PUC Docket No. L-2022-3034353, at 9 (Feb. 8, 2023).

To further enhance and deepen the discussion, the Commission is including, as Appendix B to this Order, Staff's current draft working proposal for new and modified cybersecurity fitness and cyber incident reporting regulations. The Commission clarifies that as part of the ANOPR process, these proposed regulations are providing further context for the regulated community to comment. Commenters are encouraged to reference the Staff Working Proposals in developing their comments.

In summary, the Staff Working Proposals are as follows:

Amend existing regulations at 52 Pa. Code §§ 57.11, 59.11, 61.11 and 65.2 (each relating to accidents):

- Eliminate current accident reporting requirements as they relate to cyber attacks, for electric distribution, gas, steam and water utilities.
- Preserve current accident reporting requirements as they relate to events other than cyber attacks.

Amend existing Chapter 101 (relating to public utility preparedness through self certification):

- Eliminate the Self Certification Form and related reporting requirements.
- Eliminate references and requirements relating to Cyber Security and a Cyber Security Plan.
- Preserve requirements relating to a jurisdictional utility's physical security plan, emergency response plan and business continuity plan.

Create a new Chapter 103 (relating to cybersecurity assessments, programs, standards and plans):

- Organizes public utilities into five classes for purposes of cybersecurity programs, plans and standards.

- Requires public utilities to file an annual certification that it maintains and conforms to applicable cybersecurity standards including, for larger public utilities, the NIST Cybersecurity Framework, NIST Special Publication 800-53 and NIST Special Publication 800-82.
- Provides for public utilities to seek a waiver of cybersecurity standards and related requirements when the utility can demonstrate the appropriate level of cybersecurity fitness.
- Provides for updating of third-party standards in the Commission's regulations.
- Provides for enforcement of cybersecurity standards and related requirements.

Create a new Chapter 104 (relating to cybersecurity incident reporting):

- Requires a public utility to report cyber incidents to the Commission in specified circumstances.
- Provides a time frame and a method for a public utility to report a cyber incident.

Interested parties will have 60 days from the date of publication of the Supplemental ANOPR in the *Pennsylvania Bulletin* for the submission of comments. Comments should be clearly delineated as responding to one or more of the numbered topics listed in Appendix A to this Supplemental ANOPR. Comments should include, where appropriate, a numerical reference to the existing regulation or regulations, and/or the Staff Working Proposals, which the comments address, the proposed language for revision, and a clear explanation for the recommendation. Matters not responding to a numbered topic in Appendix A or to an existing regulation should be clearly delineated as new subjects. The Commission remains committed to completing any revisions to its regulations in a timely fashion.

THEREFORE,

IT IS ORDERED:

1. That this Supplemental Advance 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.

2. That the Secretary shall serve this Supplemental Advance Notice of Proposed Rulemaking Order on the Office of Consumer Advocate and the Office of Small Business Advocate.

3. That the Law Bureau shall deliver this Supplemental Advance Notice of Proposed Rulemaking Order to the Governor's Office of the Budget.

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

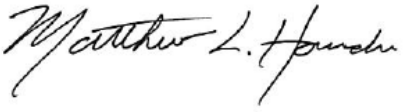
5. That, after this Supplemental Advance Notice of Proposed Rulemaking has been published in the *Pennsylvania Bulletin*, interested parties may submit written comments, referencing Docket No. L-2022-3034353, within 60 days from the date this Supplemental Advance Notice of Proposed Rulemaking Order is published in the *Pennsylvania Bulletin*. Comments may be filed either through the Public Utility Commission's e-Filing system or by mail.

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. The contact persons for this matter are Colin Scott, Assistant Counsel, Law Bureau, (717) 783-5949, colinscott@pa.gov; Chris Van de Verg, Deputy Chief Counsel, Law Bureau, (717) 783-3459, cvandeverg@pa.gov; Daniel Searfoorce, Manager—Water, Reliability and Emergency Preparedness Division, Bureau of Technical Utilities Services, (717) 783-6159, dsearfoorc@pa.gov; and Michael Holko, Director, Office of Cybersecurity Compliance and Oversight, (717) 425-5327, miholko@pa.gov. Karen Thorne, Law Bureau, kathorne@pa.gov, is the Regulatory Review Assistant for this matter.

8. That copies in Word®-compatible format of all filings at this docket shall be provided by email to the contact persons for this matter.

BY THE COMMISSION



Matthew L. Homsher
Secretary

(SEAL)

ORDER ADOPTED: April 24, 2025

ORDER ENTERED: April 24, 2025

Appendix A

Topics for Comment

Cybersecurity Fitness Standards

1. Should the Commission require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks such as NIST Cybersecurity Risk Framework, NIST Special Publication 800-53, and/or NIST Special Publication 800-82?
2. If the Commission does require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks:
    a. Should the Commission consider the extent and burden of the requirement(s) in relation to the size of the utility? If so, what criteria might the Commission use to classify utilities for purposes of differentiating their respective obligations when it comes to a utility's size and capabilities?
    b. Should the Commission specify the criteria it would consider in a petition to waive such requirements?
    c. Should the Commission enable utilities to request waivers for the use of cybersecurity programs and plans that utilize equal or stricter standards and frameworks?
    d. Should the Commission enable smaller utilities with less critical infrastructure to request waivers to specific standards and frameworks if they can demonstrate that they do not apply to them?
    e. How should the Commission account for changes and updates to those standards and frameworks over time?
    f. How should the Commission confirm compliance with those requirements?
    g. How should the Commission enforce those requirements in the event of violations?
3. Should an annual certification by a public utility that it adheres (or does not adhere) to a specific cybersecurity standard be considered confidential security

information (CSI) pursuant to Pennsylvania's *Public Utility Confidential Security Information Disclosure Protection Act*, 35 P.S. § 2141.1—2141.6 (CSI Act).

4. If an annual certification should be considered CSI, what procedures should the Commission follow to securely accept electronic filing of certifications consistent with the CSI Act?

Cyber Incident Reporting

5. Are the purposes and design for cyber incident report collection stated by CISA, NOPR at Section III.C. ("Purpose of Regulation"), substantially the same as the Commission's statutory role in ensuring that jurisdictional utilities provide reasonably adequate, reliable, continuous and safe service to the public?
6. Identify any role you believe the Commission has to play in each of the following areas:
    a. Trend and threat analysis (i.e., the performance of cybersecurity threat and incident trend analysis and tracking, to include the analysis and identification of adversary tactics, techniques, and procedures (TTPs)).
    b. Vulnerability and mitigation assessment (i.e., the identification of cyber vulnerabilities and the assessment of countermeasures that might be available to address them).
    c. The provision of early warnings (i.e., the rapid sharing of information on cyber threats, vulnerabilities, and countermeasures through the issuance of cybersecurity alerts or other means).
    d. Incident response and mitigation (i.e., rapid identification of significant cybersecurity incidents and offering of assistance—e.g., personnel, services—in incident response, mitigation, or recovery).
    e. Supporting Federal efforts to disrupt threat actors; and advancing cyber resiliency (i.e., developing and sharing strategies for improving overall cybersecurity resilience; facilitating use of cyber incident data to further

cybersecurity research; engagement with software/equipment manufacturers on vulnerabilities and how to close them).

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?

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

8. Should the PUC accept incident reports submitted by a public utility to comply with another agency's regulations and if so, describe how the process could work?

Eliminating Regulatory Duplication and Overlap

9. Given that nothing in CIRCIA or CISA's NOPR to implement CIRCIA contemplates CISA sharing any cyber incident information with the Commission, explain whether and how CIRCIA and/or CISA implementation of CIRCIA nevertheless create a potential for regulatory duplication or overlap?

10. If the Commission does require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks, how should the Commission eliminate regulatory duplication or overlap?

General

11. Would the elimination of the cybersecurity aspects of Chapter 101 of the PUC's regulations, as set forth in the Staff Working Proposals, impact the physical security, emergency response and/or business continuity aspects of the rule and/or Chapter 101 generally? The PUC seeks comments on the nature and extent of such foreseeable impacts and ways to address those impacts.

12. Comment on how the costs and benefits associated with the Staff Working Proposals can be objectively quantified and evaluated pursuant to the Pennsylvania Regulatory Review Act, 71 P.S. §§ 745.1, *et seq*.
13. Comment as to any additional considerations that you may wish to raise at this time relating to PUC oversight and regulation of public utilities as it relates to their cybersecurity fitness and/or cyber incident reporting.

Appendix B

Staff Working Proposals

§ 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 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 electrified facilities.

(d) *Telephone reports.* A report by telephone **[shall] must** 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] must** 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] must** 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] must** 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] must** 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] must** 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] must** 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 **[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, 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]**__**must**__ 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 __**steam**__ utility facilities unless a vehicle involved in the accident is owned by the steam utility or driven by a __**steam**__ utility employee while on duty.

(d) *Telephone reports.* A report by telephone **[shall]** __**must**__ 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]** __**must**__ 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]** __**must**__ 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 __**steam**__ 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] must** 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.

§ 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]must** 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]must** 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]must** 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]must** 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.]

(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).]**

(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 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.

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:

- Social Security number.
- Driver's license number or a State identification card number issued in lieu of a driver's license.
- 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.
- Medical information.

- Health insurance information.
- 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:

- IT, OT, and cloud environment architectural reviews are completed prior to implementation to ensure they comply with the utility's governance policies and procedures.
- 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.
- Changes to system configurations and patch management processes and procedures are documented and system operators are made aware of these changes.
- All confidential data is encrypted at rest and in transit.
- All network traffic is documented, and proper security mechanisms are in place to protect the internal and external networks.
- All physical access controls are documented and monitored and comply with applicable standards.

- 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.

103.2 Cybersecurity Evaluations and Programs

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

(i) An annual cybersecurity evaluation which:

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

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

(1) NIST CSF,

(2) NIST Special Publication 800-53, and

(3) NIST Special Publication 800-82.

(ii) A governance program.

(iii) A security management program.

(iv) A vulnerability management program.

(v) A risk management program.

(vi) A threat management program.

(vii) An incident response program.

(viii) A recovery management program.

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

(i) An annual cybersecurity evaluation which:

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

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

(ii) A governance program.

(iii) A security management.

(iv) A vulnerability management program.

(v) A risk management program.

(vi) A threat management program.

(vii) An incident response program.

(viii) A recovery management program.

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

(i) An annual cybersecurity evaluation which:

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

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

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

(iii) An annual vulnerability assessment.

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

(v) 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.

(vi) A COOP.

(vii) a disaster recovery plan.

(d) a telecommunications utility shall develop and maintain a written cybersecurity plan, which 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 telecommunications utility could no longer continue to operate.

103.3 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 § 103.2(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 § 103.2(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 § 103.2(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 § 103.2(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.

103.4 Waiver.

A public utility may petition the Commission for a waiver from any of the cybersecurity evaluation or program standards set forth in section 103.2(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. If the Commission grants the petition, it may require the public utility to file with the Commission on an annual basis an appropriate certification that the public utility maintains and conforms to its exempted cybersecurity program.

103.5 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. Comments may be filed with the Commission no later than 30 days following publication of the Commission notice in the *Pennsylvania Bulletin*.

(d) An update under paragraph (a) that is the subject of a Commission notice pursuant to paragraph (c) shall become effective 120 days after publication of the notice in the *Pennsylvania Bulletin* unless the Commission determines otherwise for good cause shown.

103.6 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).

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 Requirement

(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 network 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 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 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 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 shall report a cyber incident that meets one or more of the criteria in subsection (a) of this Section to the PaCIC and shall provide verbal confirmation to the Commission-designated representative of same.