PENNSYLVANIA
PUBLIC UTILITY COMMISSION
Harrisburg PA 17105-3265

Public Meeting held November 10, 2022

Commissioners Present:

Gladys Brown Dutrieuille, Chairman
Stephen M. DeFrank, Vice Chairman
Ralph V. Yanora
Katie L. Zerfuss
John F. Coleman, Jr.

Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting	L-2022-3034353

ADVANCE NOTICE OF PROPOSED RULEMAKING ORDER

BY THE COMMISSION:

The Pennsylvania Public Utility Commission (PUC) enters this Advance Notice of Proposed Rulemaking Order (ANOPR) to review its current regulations relating to cybersecurity.[1] 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, and
- 65.2 (relating to accidents) for water public utilities.

[1] The Commission's existing regulations use "cyber security" in lieu of the widely accepted "cybersecurity." For purposes of this ANOPR, "cybersecurity" shall be used, except when quoting directly from the existing regulations.
[2] The Commission's prior orders use "cyber attack" whereas its existing regulations use "cyber-attack." For purposes of this ANOPR, "cyber attack" shall be used, except when quoting directly from the existing regulations.

Self-certification regulations include:

- 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.

The PUC seeks comments from interested stakeholders, including members of the regulated industry, statutory advocates, the public, and any other interested parties about whether the existing regulations are sufficient or if they need to be revised to ensure that they address public utility fitness in the current and anticipated future cybersecurity threat landscapes. Throughout this ANOPR, any proposed changes, consolidations, deletions, and additions to the existing regulations shall be referred to as "revisions."

BACKGROUND

The PUC's Self-Certification Regulations

The self-certification regulations were first promulgated in 2005 to require "all jurisdictional utilities to develop and maintain written physical, cyber security, emergency response and business continuity plans to protect the Commonwealth's infrastructure and ensure safe, continuous and reliable utility service."[3] These regulations grew out of the PUC's efforts to coordinate its security efforts with the Pennsylvania Office of Homeland Security and thereby to develop a security self-certification process for all jurisdictional utilities.[4] The PUC endeavored not to replicate regulations that were already in place and required by the Federal government or other agencies but acknowledged its duty to identify and secure critical utility infrastructure and key assets within the Commonwealth.[5]

---

[3] 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).
[4] *Id*. at 2.
[5] *Id*. at 24.

In summary, 52 Pa. Code § 101.1 (relating to purpose) requires every "jurisdictional utility" to "develop and maintain" a cybersecurity plan "to protect this Commonwealth's infrastructure and ensure safe, continuous and reliable utility service."[6] To ensure compliance, a jurisdictional utility annually submits a Self -Certification Form (SCF) stating that it has a cybersecurity plan in place which the PUC may review upon request.[7] Per 52 Pa. Code § 101.2 (relating to definitions), "jurisdictional utility" is defined to include only those utilities which file annual reports under the following provisions:

- 52 Pa. Code §§ 27.10 (relating to accounts, records and reports) for air transportation utilities,
- 29.43 (relating to assessment reports) for motor vehicle common carriers,
- 31.10 (relating to assessment reports) for motor common carriers of property,
- 33.103 (relating to reports) for railroad carriers,
- 57.47 (relating to filing of annual financial reports) for electricity public utilities,
- 59.48 (filing of annual financial reports) for gas public utilities,
- 61.28 (filing of annual financial reports) for steam utilities,
- 63.36 (relating to filing of annual financial reports) for telecommunications public utilities, and
- 65.19 (relating to filing of annual financial reports) for water public utilities.

By contrast, certain public utilities and licensed entities under the PUC's supervision do not qualify as a "jurisdictional utility" under Section 101.2 and are thus not subject to the existing self-certification regulations, including but not limited to electric generation

[6] Section 101.1 also requires jurisdictional utilities to develop and maintain plans for physical security, emergency response and business continuity.
[7] *See generally* 52 Pa. Code §§ 101.1–101.7 (relating to public utility preparedness through self-certification) (Chapter 101).

suppliers (EGS), natural gas suppliers (NGS), transportation network companies (TNCs) and wastewater public utilities.

The PUC's Existing Cyber Attack Reporting Regulations

The PUC promulgated cyber attack reporting regulations for electric, gas and water public utilities in 2011, as part of a broader effort to "establish a more uniform approach to reportable accidents involving utility facilities and operations."[8] These regulations resulted from consumer dissatisfaction with electric public utilities' service restoration and public notice practices in the wake of Hurricane Ike, which swept through Pennsylvania in 2008, interrupting electric service to more than 450,000 customers.[9]

As it relates to cybersecurity, the PUC broadened the scope of the previously existing cyber attack reporting regulations for electric, gas and water public utilities to include "an occurrence of an unusual nature that is a physical or cyber-attack, including attempts against cyber security measures as defined in Chapter 101 that causes an interruption of service or over $50,000 in damages, or both."[10] Section 101.2 defines "cyber security" as "[t]he measures designed to protect computers, software and communications networks that support, operate or otherwise interact with the company's operations."

The PUC reasoned that since it "only requires reporting if the cyber attack causes an interruption of service and/or over $50,000 in damages, . . . the reporting requirement will be less burdensome than reporting any cyber attack."[11] The PUC further reasoned that "the $50,000 threshold is high enough to prevent reporting minor everyday

---

[8] Final Rulemaking Order, *Proposed Rulemaking for Revision of 52 Pa. Code Chapters 57, 59, 65 and 67 Pertaining to Utilities' Service Outage Response and Restoration Practices*, Pa. P.U.C. Docket No. L-2009-2104274 (order entered Sept. 23, 2011) at 3, 42 Pa.B. 9 (Jan. 7, 2012) (Outage Response Order).
[9] *Id*. at 2.
[10] *See* 52 Pa. Code §§ 57.11(b)(4), 59.11(b)(5) and 65.2(b)(4).
[11] *Outage Response Order* at 10.

occurrences but still allows the PUC to have knowledge of incidences that result in a significant expense."[12]

The PUC's Existing Cybersecurity Regulations for Steam Utilities

Self-certification and cyber attack reporting regulations relative to steam utilities were added in 2017 as part of a broader initiative "to modernize and update its existing steam heat regulations and to add steam heat safety regulations…."[13] This initiative resulted from a 2007 steam pipeline explosion in New York City and inquiries into steam pipeline safety in the Commonwealth by members of the General Assembly.

As they relate to cybersecurity, the steam utilities rulemaking resulted in two new sets of obligations. First, steam public utilities were required to report accidents involving "[a]n 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."[14] Notably, this cyber attack reporting requirement differs significantly from the requirement for electric, gas and water public utilities. For example, there is no reference to interruption of service or $50,000 in damages.

Second, steam utilities were required to "develop and maintain written plans for physical and cyber security, emergency response and business continuity in accordance with § 101.3 (relating to plan requirements)."[15]

---

[12] *Id*.
[13] Final Rulemaking Order, *Final Rulemaking Re Steam Heat Distribution System Safety Regulations*, 52 Pa. Code Chapters 61 and 67, Pa. P.U.C. Docket No. L-2015-2498111 at 3 (Order entered Aug. 3, 2017), 47 Pa.B. 48 (Dec. 2, 2017) (Steam Utilities Order).
[14] 52 Pa. Code § 61.11(b)(6).
[15] 52 Pa. Code § 61.45(a).

Statutory Basis for New or Revised Cybersecurity Regulations

The statutory bases for both the cyber attack reporting regulations and the self-certification regulations are Sections 501, 504, 505, 506, and 1501 of the Public Utility Code, 66 Pa.C.S. §§ 501, 504, 505, 506 and 1501.[16]

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

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

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

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

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

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

> any portion thereof, and shall furnish any and all other information to the commission, as the commission may require, in any inspection, examination, inquiry, investigation, hearing, or determination of such value of its property, or any portion thereof.

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

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

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

> Every public utility shall furnish and maintain adequate, efficient, safe, and reasonable service and facilities, and shall make all such repairs, changes, alterations, substitutions, extensions, and improvements in or to such service and facilities as shall be necessary or proper for the accommodation, convenience, and safety of its patrons, employees, and the public.

The cyber attack reporting regulations also rely on 66 Pa.C.S. § 3009(b) and (d).[17] However, Section 3009 was repealed by Section 1 of the act of November 30, 2004 (P.L. 1398) and replaced by 66 Pa.C.S. § 3019 (relating to additional powers and duties).

[17] Outage Response Order at 36.

The regulations for steam utilities are authorized by Sections 501 and 1501.[18]

DISCUSSION

The PUC faces several considerations in preparing to potentially update and revise its existing cybersecurity regulations.

Updating Terms and Concepts

Section 101.2 defines "cyber security" as "[t]he measures designed to protect computers, software and communications networks that support, operate or otherwise interact with the company's operations" and "cyber security plan" as "[a] written plan that delineates a jurisdictional utility's information technology disaster plan."

The PUC's industry-specific cyber attack reporting regulations do not contain definitions of their own but instead rely on Chapter 101. For example, Section 57.11(b)(4), applicable to electric public utilities, defines "reportable accident," in pertinent part, as "[a]n 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."

Contemporary definitions of these and similar terms have evolved greatly since 2005 and incorporate now-standard concepts such as the "CIA Triad."[19] For example, the National Institute of Standards and Technology (NIST) defines "cybersecurity" as "[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and

[18] Steam Utilities Public Order at 22.
[19] CIA Triad refers to the concept of designing cybersecurity measures and systems to protect the confidentiality, integrity, and availability of information.

electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[20]

Similarly, in contemporary parlance, "cybersecurity plan" could refer to either or both of the following:

- A document that sets forth the organization's overall strategy to identify the desired level of cybersecurity fitness and address cybersecurity gaps.
- An operational plan which details the precise measures to be implemented to address specific cybersecurity objectives.

Additionally, a document that sets forth the organization's overall strategy to identify the desired level of cybersecurity fitness and address cybersecurity gaps may be referred to as a "cybersecurity program."

Finally, the existing regulations include terms such as "cyber attack" and "cyber security measures," without clearly defining them or distinguishing them from related, commonly used terms such as "cyber incident" and "cyber risk."[21]

The PUC seeks comment on whether and how to update the terms and concepts used in the existing regulations to better reflect the current cybersecurity landscape, Federal and industry standards and any revisions which may be adopted in this rulemaking.

---

[20] NIST, Computer Security Resource Center (CSRC), *Glossary*, available online at: https://csrc.nist.gov/glossary/term/cybersecurity (last accessed on Oct. 24, 2022).
[21] *Id.*, available online at: https://csrc.nist.gov/glossary/term/cyber_incident and https://csrc.nist.gov/glossary/term/cyber_risk (last accessed on Oct. 24, 2022).

Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities

The overriding purpose of the PUC's existing self-certification regulations is "to protect this Commonwealth's infrastructure and ensure safe, continuous and reliable utility service."[22] However, the existing regulations' central cybersecurity plan requirement, 52 Pa. Code § 101.4, focuses on just four basic security controls: (1) identifying "[c]ritical functions requiring automated processing"; (2) "[a]ppropriate backup for application software and data"; (3) "[a]lternative methods for meeting critical functional responsibilities in the absence of information technology capabilities"; and (4) "[a] recognition of the critical time period for each information system before the utility could no longer continue to operate."

Since the self-certification regulations were first drafted by the PUC in 2005, cyber threats have continuously evolved and increased in number, type, and sophistication. Today, ransomware attacks prevail as a leading form of cyber threat. Ransomware is a type of malware, or malicious software, that encrypts a victim's data or computing device and threatens to keep it encrypted unless the victim pays the attacker a ransom. Ransomware can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Ransomware attacks have, in recent years, increasingly targeted critical infrastructure and government agencies.[23]

Another growing cyber threat is the potential for attacks on public utilities' operational technology (OT), the hardware and software that control the physical equipment and systems with which utilities provide service. Public utilities have been working hard to integrate information technology (IT) and OT systems as part of grid modernization. This IT-OT interdependence creates business, environmental and

---

[22] 52 Pa. Code § 101.1 (relating to purpose).
[23] Cybersecurity & Infrastructure Security Agency, *Ransomware Guide*, available online at: https://www.cisa.gov/stopransomware/ransomware-guide (last accessed on Oct. 25, 2022).

operational benefits but also increases cyber risk. Cyber attacks on OT are intended to disrupt operations, damage critical equipment, and even inflict bodily harm.[24]

The steady rise in the creativity, number and severity of cyber attacks raises the bar for cybersecurity. Industry and government have continuously reviewed, expanded and improved cybersecurity standards for entities of all kinds. At the federal level, the National Institute for Standards and Technology (NIST) has led the way in the advancement of cybersecurity standards. NIST's Cybersecurity Framework, with its five-functions approach (identify, protect, detect, respond and recover) provides a model and a process to increase cybersecurity maturity in any organization.[25]

Taking a more granular approach, NIST Special Publication 800-82 (Guide to Industrial Control Systems (ICS) Security) provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. NIST 800-82 provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.[26]

---

[24] Forbes, *Defending Against Cyberattacks on Operational Technology*, by Ryan Moody (Oct. 28, 2021), available online at: https://www.forbes.com/sites/forbestechcouncil/2021/10/28/defending-against-cyberattacks-on-operational-technology/?sh=7418675c5e76 (last accessed Oct. 25, 2022).
[25] NIST, *Cybersecurity Framework*, available online at: https://www.nist.gov/cyberframework (last accessed Oct. 24, 2022).
[26]NIST, Special Publication 800-82, Rev. 2, *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*, (May 2015), available online at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (last accessed Oct. 25, 2022).

At the most prescriptive end of the spectrum, the North American Electric Reliability Corporation Critical Infrastructure Protection Standards (CIP Reliability Standards) are designed to address the evolving nature of cyber-related threats to the bulk power system. Although called "standards", the CIP Reliability Standards are developed by NERC and become mandatory and enforceable after approval the Federal Energy Regulatory Commission (FERC) and apply to users, owners and operators of the bulk power system, as set forth in each of the thirteen (13) current standards. The CIP Reliability Standards require certain users, owners, and operators of the bulk power system to comply with specific requirements to safeguard critical cyber assets. These standards are results-based and do not specify a technology or method to achieve compliance, instead leaving it up to the utility to decide how best to comply with the standards.[27]

Based on the variety of approaches taken by regulators at the Federal level, it appears that the PUC has, at a minimum, five potential regulatory approaches to ensure that public utilities have adequate cybersecurity plans in place to respond to cyber threats:

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

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

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

[27] FERC, *Cybersecurity Incentives Policy White Paper* (June 2020), at 4-8, available online at: https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf (last accessed Oct. 25, 2022).

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

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

The PUC seeks comment on the relative merits and weaknesses of each of the above approaches and which of these approaches, some combination of these approaches, or some other approach, provides the PUC, the public utility and its ratepayers with the greatest potential assurance that the utility is adequately prepared to address cybersecurity threats. Similarly, the PUC welcomes comments describing the approaches taken by other state public utility commissions to address public utilities' cybersecurity fitness and evaluating their respective costs and benefits.

Section 101.3 requires that "[a] jurisdictional utility shall develop and maintain written physical and cyber security, emergency response and business continuity plans." This ANOPR focuses on the cybersecurity component of this rule. However, it is possible that changes to the cybersecurity aspect of this regulation could impact the physical security, emergency response, or business continuity requirements of Section 101.3 or any of the rest of Chapter 101. The PUC seeks comment on the nature and extent of such foreseeable impacts and ways to address those impacts.

Section 101.2 applies to jurisdictional public utilities, including many classes of certificated public utilities under the PUC's jurisdiction, but does not apply to other entities under the PUC's supervision, such as EGS, NGS and TNC entities. The PUC seeks comment on whether the self certification regulations, or revisions thereto, should be applied to additional types of entities that are subject to the PUC's supervision.

Conversely, the PUC's current self-certification regulations apply equally to widely disparate types of public utilities, some of which are highly sophisticated corporate conglomerates which operate first-tier critical infrastructure and others of which are sole proprietorships and small businesses offering a limited class of service that does not implicate critical infrastructure. The PUC seeks comment as to whether there are public utility types which should be wholly or partially exempt from the self-certification, based on easing the regulatory burden on small businesses, or for other reasons.

Improving the Self-Certification Form (SCF) Process

Since the initial promulgation of the self-certification regulations, the PUC has experienced issues regarding the SCF: how it is processed, confidentiality of the information collected, and impact on smaller utilities. Concerns have also emerged with respect to the self-certification form's value to assessing and ensuring public utilities' cybersecurity fitness.

Processing the SCF is a complex matter. Section 101.5 states that an SCF filed at the PUC "is not a public document or record and is deemed confidential and proprietary." Further, the information contained in an SCF may constitute Confidential Security Information (CSI), which means that SCFs must be submitted on paper and filed with the Secretary's Bureau to ensure their receipt and storage comply with Pennsylvania's CSI law[28] and the PUC's implementing regulations.[29]

Treating the SCFs as CSI impacts how the information on the form is stored, accessed, and validated once filed. These additional security protocols lead to delays and

[28] Pennsylvania Public Utility Confidential Security Information Disclosure Protection Act, 35 Pa. P.S. §§ 2141.1 — 2141.6.
[29] *See*, *e.g.*, 52 Pa. Code § 102.3 (relating to filing procedures) ("The Commission does not authorize the use of e-mail or any other electronic mail system to transmit records containing confidential security information.").

an increase in the workload for PUC staff. Adding to the complexity of processing the form, Section 101.4(a) requires that some public utilities file this form at the same time they file their Annual Financial Report, which is due annually at the end of April, while Section 101.4(b) directs other public utilities to file the form with their Annual Assessment Report, which is due annually at the end of March.

The PUC seeks comment on ways to streamline and otherwise improve the filing, handling, and storage of SCFs.

The self-certification regulations apply the same standards to almost all public utilities, including more than 7,500 transportation public utilities including Amish ride services, taxis, limousines, ambulance companies, towing services, and moving companies. PUC staff routinely receives questions from transportation public utilities questioning why they are receiving the form and looking for guidance on how the regulations apply to small companies without an IT department. Small transportation public utilities also ask why they need to have a cybersecurity plan, a disaster recovery plan, and a business continuity plan when their core business function is transporting individuals, small groups, or commodities.

Thus, it may be that, in the case of some public utility types, the administrative costs of maintaining the existing self-certification regulations may exceed any cybersecurity benefit the existing regulations may impart. Alternatively, it might be preferable for the PUC to apply the existing regulations, or revisions thereto, in a granular manner, applying different reporting requirements for public utilities that meet certain criteria.

The PUC seeks comment on whether and how to streamline the self-certification form, plan, and reporting requirements to better calibrate the benefits of the existing

regulations against the burdens they place on regulated entities, especially smaller utilities, and on PUC staff.

Updating Cyber Attack Reporting Regulations

The PUC promulgated regulations in 2011 that require Pennsylvania's regulated electric, natural gas and water public utilities to report physical or cyber attacks that cause either or both an interruption of service or $50,000 in damages.[30] These standards focus on interruption of service as a criterion for reporting, thereby implicating the facilities that provide service to customers, otherwise known as OT.

However, since 2011, the afore-mentioned convergence of IT and OT in the utility industry increases the risk of cyber threats arising in the IT environment threatening OT. In colloquial terms, the "air gap" which once existed between OT systems which provide service and the IT systems which monitor, and control OT, is disappearing.

An IT incident can escalate quickly and lead to service outages that may trigger a response by the PUC and other critical infrastructure stakeholders such as the Pennsylvania Emergency Management Agency (PEMA), Pennsylvania Army National Guard (PANG), Pennsylvania State Police (PSP) and Pennsylvania Governor's Office of Homeland Security (GOHS). These government agencies stand ready assist Commonwealth residents with access to critical services like water, electricity, natural gas, food, and shelter until the incident is resolved. The PUC is also a stakeholder affecting any public utility service in Pennsylvania and therefore needs to have advance warning of threats emerging in the IT environment.

[30] *See*, *e.g.*, 52 Pa. Code § 57.11(b)(4).

The PUC seeks comment on potential ways to revise the reporting criteria in its existing regulations, including the potential addition of new requirements for reporting incidents involving IT.

Another cyber attack reporting issue to explore is whether the $50,000 criterion should be revised. The existing regulations do not address how a public utility should attribute damages to a cyber attack, what costs should be considered as damages, whether the availability of insurance is relevant or when the damages calculation should be performed. This ambiguity may lead public utilities to spend inordinate efforts attempting to perform the calculation or conversely even not reporting serious incidents at all simply because there is no clearly defined financial impact.

The PUC seeks comment with respect to the continuing efficacy of the $50,000 reporting threshold.

Merging the Self-Certification and Cyber Attack Reporting Regulations

Given the growth in cybersecurity as an area of concern, it may be preferable that all the PUC's cybersecurity regulations be handled in the same chapter of the PUC's regulations. Further, there does not appear to be a compelling reason to maintain different reporting thresholds for steam public utilities as is applied to the other public utilities for which reporting is required. Finally, there is an open question as to whether the reporting requirements should remain limited to water, electric, gas and steam public utilities, or be broadened to include any of the following: other certificated public utilities, such as wastewater and telecommunications public utilities, and licensed entities such as those providing EGS, NGS and TNC services.

For ease of reference and clarity of purpose, the current cyber attack reporting regulations could be removed from the various industry-specific provisions of the PUC's regulations where they are currently located and consolidated in a new chapter or as a

new section within Chapter 101. The PUC seeks comment on the pros and cons of merging the self-certification and cyber incident reporting regulations into a single chapter of the Code, and otherwise eliminating unintended or unjustified inconsistencies in the existing regulations.

Cost-Benefit Analysis

Any revisions to the existing regulations must be deemed to be in the public interest in order to be approved prior to promulgation. Under the Regulatory Review Act, 71 P.S. §§ 745.1, *et seq*., the statutory criteria to evaluate if a regulation is in the public interest are:

> (1) Economic or fiscal impacts of the regulation, which include the following:
>
> > (i) Direct and indirect costs to the Commonwealth, to its political subdivisions and to the private sector.
> >
> > (ii) Adverse effects on prices of goods and services, productivity or competition.
> >
> > (iii) The nature of required reports, forms or other paperwork and the estimated cost of their preparation by individuals, businesses and organizations in the public and private sectors.
> >
> > (iv) The nature and estimated cost of legal, consulting or accounting services which the public or private sector may incur.
> >
> > (v) The impact on the public interest of exempting or setting lesser standards of compliance for individuals or small businesses when it is lawful, desirable and feasible to do so.
>
> (2) The protection of the public health, safety and welfare and the effect on this Commonwealth's natural resources.
>
> (3) The clarity, feasibility and reasonableness of the regulation to be determined by considering the following:

(i) Possible conflict with or duplication of statutes or existing regulations.

(ii) Clarity and lack of ambiguity.

(iii) Need for the regulation.

(iv) Reasonableness of requirements, implementation procedures and timetables for compliance by the public and private sectors.

(v) Whether acceptable data is the basis of the regulation.

(4) Whether the regulation represents a policy decision of such a substantial nature that it requires legislative review.

(5) Comments, objections or recommendations of a committee.

(6) Compliance with the provisions of this act or the regulations of the commission in promulgating the regulation.

(7) Whether the regulation is supported by acceptable data.

(8) Whether a less costly or less intrusive alternative method of achieving the goal of the regulation has been considered for regulations impacting small business.

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

Eliminating Regulatory Duplication and Overlap

The PUC's existing cybersecurity regulations do not exist in a vacuum. Federal and state cybersecurity, incident reporting, and data privacy laws and regulations have proliferated over the last decade or more since the PUC's regulations were first promulgated. The process of deconflicting regulations that duplicate, contradict or overlap each other has become an art unto itself.

Section 101.6(d) currently addresses this deconfliction. First, it provides that a public 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 that plan for compliance with this subpart, upon the condition that a [PUC] representative be permitted to review the cyber security, physical security, emergency response or business continuity plan."

Second, Section 101.7 by its own terms "does not apply to an entity regulated by the Federal Railroad Safety Act (FRSA) (49 U.S.C. §§ 20101–20153) and the Hazardous Materials Transportation Act (HMTA) (49 U.S.C. §§ 5101–5127), if by August 10, 2005, it submits a certification to the [PUC] 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."

In the realm of cyber incident reporting, the PUC notes Congress' recent enactment of the Federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[31] CIRCIA provides for critical infrastructure operators to report covered cybersecurity incidents to the Federal Cybersecurity and Infrastructure Security Agency (CISA). CIRCIA reflects a comprehensive, state-of-the-art approach to critical infrastructure cybersecurity. CIRCIA's focus on the interaction between and among IT, OT and third-party supply chains may serve as a model for the PUC's cyber incident reporting regulations. Further, depending on the outcome of its rulemakings, CISA may designate any or all critical infrastructure sectors, including communications, energy and water and wastewater systems sectors as covered by CIRCIA's reporting requirements.

[31] 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*.)

The PUC seeks comment on the potential for conflict, overlap, redundancy, or other bases warranting review in the interplay between the PUC's cybersecurity regulations (and revisions thereto) and Federal initiatives, including but not limited to CIRCIA.

Other Matters

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

CONCLUSION

Due to the breadth of topics addressed in this rulemaking and the potential complexity of the regulations which are open for review, interested parties will have sixty (60) days from the date of publication of the 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 ANOPR. Comments should include, where appropriate, a numerical reference to the existing regulation or regulations 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 PUC is committed to completing any revisions to its regulations in a timely fashion; **THEREFORE,**

IT IS ORDERED:

1. That an advance notice of a proposed rulemaking proceeding is hereby initiated at this docket to consider whether and how the existing regulations in Title 52 of the Pennsylvania Code relating to cybersecurity should be revised.

2. That this 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.

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

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

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

6. That, after this 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 sixty (60) days from the date this 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.

7. 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/.

8. The contact persons for this matter are Colin Scott, Assistant Counsel, Law Bureau, (717) 783-5949, colinscott@pa.gov; Chris Van de Verg, Assistant 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.

9. 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

Rosemary Chiavetta,
Secretary

(SEAL)

ORDER ADOPTED: November 10, 2022

ORDER ENTERED: November 10, 2022

Appendix A

Topics for Comment

Introduction

1. The PUC seeks comments from interested stakeholders, including members of the regulated industry, statutory advocates, the public, and any other interested parties about whether the existing regulations are sufficient or if they need to be revised to ensure that they address public utility fitness in the current and anticipated future cybersecurity threat landscapes. *See* ANOPR at 2.

Updating Terms and Concepts

2. The PUC seeks comment on whether and how to update the terms and concepts used in the existing regulations to better reflect the current cybersecurity landscape, Federal and industry standards and any revisions which may be adopted in this rulemaking. *See* ANOPR at 9.

Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities

3. The PUC seeks comment on the relative merits and weaknesses of each of the approaches within the heading "Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities" and which of these approaches, some combination of these approaches, or some other approach, provides the PUC, the utility and its ratepayers with the greatest potential assurance that a utility is adequately prepared to address cyber security threats. *See* ANOPR at 13.

4. The PUC welcomes comments describing the approaches taken by other state public utility commissions to address public utilities' cybersecurity fitness and evaluating their respective costs and benefits. *See* ANOPR at 13.

5. Would changes to the cybersecurity aspect of 52 Pa. Code § 101.3 impact the physical security, emergency response and/or business continuity aspects of the rule and/or Chapter 101 generally? The PUC seeks comment on the nature and

extent of such foreseeable impacts and ways to address those impacts. *See* ANOPR at 13.

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

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

Improving the Self-Certification Form (SCF) Process

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

9. The PUC seeks comment on whether and how to streamline the self-certification form, plan and reporting requirements to better calibrate the benefits of the existing regulations against the burdens they place on regulated entities, especially smaller utilities, and on PUC staff. *See* ANOPR at 15-16.

Updating Cyber Attack Reporting Regulations

10. The PUC seeks comment on potential ways to revise the reporting criteria in its existing regulations, including the potential addition of new requirements for reporting incidents involving IT. *See* ANOPR at 17.

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

Merging the Self-Certification and Cyber Attack Reporting Regulations

12. The PUC seeks comment on the pros and cons of merging the self-certification and cyber incident reporting regulations into a single chapter of the Code, and otherwise eliminating unintended or unjustified inconsistencies in the existing regulations. *See* ANOPR at 18.

Cost-Benefit Analysis

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

Eliminating Regulatory Duplication and Overlap

14. The PUC seeks comment on the potential for conflict, overlap, redundancy, or other bases warranting review in the interplay between the PUC's cybersecurity regulations (and revisions thereto) and Federal initiatives, including but not limited to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). *See* ANOPR at 21.

Other Matters

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