Suzan D. Paiva
Associate General Counsel

900 Race Street, 6th Floor
Philadelphia, PA 19107
suzan.d.paiva@verizon.com

July 16, 2025

VIA ELECTRONIC FILING

Matthew L. Homsher, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor
Harrisburg, PA 17120

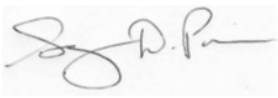
RE: Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting; Supplemental Advance Notice of Proposed Rulemaking
Docket No. L-2022-3034353

Dear Secretary Homsher:

Enclosed please find Verizon's Supplemental Comments in response to the April 24, 2025 Supplemental Advance Notice of Proposed Rulemaking Order in the above captioned matter.

Please do not hesitate to contact me with any questions.

Very truly yours,



Suzan D. Paiva

Via Email

cc: Colin Scott, Assistant Counsel, Law Bureau (colinscott@pa.gov)
Chris Van de Verg, Assistant Counsel, Law Bureau (cvandeverg@pa.gov)
Daniel Searfoorce, Manager, Bureau of Technical Utilities Services (dsearfoorc@pa.gov)
Michael Holko, Director, Office of Cybersecurity Compliance and Oversight (miholko@pa.gov)
Karen Thorne, Law Bureau (kathorne@pa.gov)

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

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

VERIZON'S SUPPLEMENTAL COMMENTS

On April 24, 2025, the Commission issued a Supplemental Advance Notice of Proposed Rulemaking Order ("Supplemental ANOPR") seeking additional comments on limited, specified topics related to potential changes to its regulations on cybersecurity self-certifications and cyber attack reporting. In response to the May 17, 2025 publication of this Supplemental ANOPR in the Pennsylvania Bulletin, Verizon[1] submits the following supplemental comments to update the background information that was provided in Verizon's February 8, 2023 comments on the original ANOPR and to answer the Commission's questions in Appendix A to the Supplemental ANOPR.

Verizon urges the Commission to continue to await the completion of the ongoing Cybersecurity and Infrastructure Security Agency (CISA)[2] rulemaking that will craft federal rules implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") for cyber incident reporting and related issues before taking any action on its own rules. With respect to the communications industry, the Commission should rely on the

---

1 These Comments are filed on behalf of the Verizon affiliated companies that are regulated by this Commission, including 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.

2 CISA is an operational component of the federal Department of Homeland Security (DHS) that works to understand, manage and mitigate risk to the nation's cyber and physical infrastructure in the public and private sector.

extensive multi-agency federal cybersecurity framework and avoid duplicative state requirements that could divert critical resources away from cyber defense.

I. Updated Background

Verizon incorporates the information provided in the "Background" section of its February 8, 2023 comments on the initial ANOPR and provides the following updates.

A. Cybersecurity Continues to be a Top Priority for Verizon and the Communications Industry.

The nature of the communications industry means that network resiliency and data integrity must be a key business and operational priority. Verizon and the communications sector have a long history of protecting against threats to customers' security and ensuring the reliability and resilience of communications services against all manner of hazards, including cyber threats. While Verizon does not advocate any changes to the Commission's rules given the ongoing federal activities, the Commission should be assured that protecting the security of our systems and networks continues to be a top priority for Verizon.

As described in its initial comments, Verizon continues to have a dedicated Chief Information Security Officer ("CISO") whose team is responsible for leading enterprise-wide information security strategy, policy, standards, architecture, and processes. Verizon's comprehensive information security program includes, among other aspects, vulnerability management, antivirus and malware protection, file integrity monitoring, encryption, and access control. The CISO leads an annual review and discussion with the full Board dedicated to Verizon's cyber risks, threats, and protections, and provides updates throughout the year as warranted.

Verizon's enterprise-wide Information Security Policy is aligned with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework 2.0, which is the most

recent version of this comprehensive industry guide designed to help organizations of all sizes and across all sectors manage and reduce their cybersecurity risks. As part of this policy, Verizon has deployed a comprehensive Enterprise Vulnerability Management (EVM) program designed to identify and protect against data security risks, including risk identification, risk detection, risk evaluation, and remediation of any vulnerabilities. Verizon collects and retains data to enhance management accountability for remediation of vulnerable assets, to assess threat trends, and for strategic planning of ongoing program improvements. Verizon also publishes an annual Data Breach Investigations Report to help our customers better understand the cybersecurity threats they may face and how to manage these risks effectively.[3]

Mindful of its role in the communications ecosystem and the importance of collaboration with both public and private stakeholders, Verizon is an active member in numerous bodies dedicated to enhancing collaboration, coordination, and communication. They include the following:

- For more than a decade, a Verizon representative has been elected to serve on the Executive Committee of the Communications Sector Coordinating Council (CSCC), which coordinates industry engagement with the U.S. government on cyber and infrastructure security.[4]
- Verizon's Chief Information Security Officer co-chaired the Federal Communications Commission's eighth Communications Security, Reliability and Interoperability Council (CSRIC). Currently, for the ninth CISRIC, a Verizon vice president of technology policy serves as a member. Multiple Verizon subject matter experts are actively engaged in the CSRIC's working groups that are underway developing and publishing key security recommendations for artificial intelligence, preparing for 6G security and reliability, and 911on all networks.[5]

---

[3] The 2025 Verizon Data Breach Investigations Report is available here: https://www.verizon.com/business/resources/reports/dbir/

[4] https://www.comms-scc.org/

[5] https://www.fcc.gov/communications-security-reliability-and-interoperability-council-ix

- Verizon is an active member and former chair of the Communications Sector Information Sharing and Analysis Center (Communications ISAC), also known as the National Coordinating Center for Communications (NCC). The Communications ISAC is a "clearinghouse" for physical and cyber alerts to the telecommunications industry and operates on a 24/7 basis. Established largely for the purpose of ensuring that the government's emergency communications capabilities could continue in the event of a nuclear war, the NCC/Comm ISAC was the first of the critical-infrastructure ISACs, setting the model that other critical-infrastructure sectors such as energy, finance and transportation later adapted to their own distinct needs.[6]

- Verizon is an active participant in CISA's Joint Cyber Defense Collaborative, a public-private partnership that proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense and response.[7]

- Verizon is an active member of CISA's ICT Supply Chain Risk Management Task Force. That includes co-chairing the Task Force's working group that is working on developing a Hardware Bill of Materials framework so purchasers of communications equipment can effectively and efficiently assess and manage supply chain risks and co-chairing a working group that updated the taskforce's Threat Scenarios Report to include artificial intelligence considerations.[8]

- Verizon representatives participate actively in the Enduring Security Framework (ESF), a public-private partnership comprised of experts from the U.S. Government as well as representatives from the Information Technology, Communications and the Defense Industrial Base sectors. It is charged with bringing together representatives from private and public sectors to work on intelligence-driven, shared cybersecurity challenges. ESF is chartered by the Department of Defense, Department of Homeland Security, Office of the Director of National Intelligence, and the IT, Communications and Defense Industrial Base Sector Coordinating Councils. The National Security Agency serves as the ESF. In the past year, ESF has published products that include techniques for addressing cybersecurity threats to network slicing and for addressing software supply chain security risks.[9]

---

6 https://www.cisa.gov/national-coordinating-center-communications

7 https://www.cisa.gov/jcdc

8 https://www.cisa.gov/ict-scrm-task-force

9 https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Cybersecurity-Partnerships/ESF/

B. There Continues to be Significant Regulatory Activity on Cybersecurity at the Federal Level.

Verizon also actively participates in the ongoing federal government cybersecurity initiatives and is subject to existing federal cyber security requirements.

Most recently, Verizon participated individually and through its trade associations in CISA's efforts to craft federal rules implementing CIRCIA. Signed into law in March of 2022, this federal statute directs CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. Verizon participated in the 2022 request for information (RFI) seeking input from stakeholders in preparation for issuing proposed rules.[10] On April 4, 2024, CISA issued a Notice of Proposed Rulemaking ("NPRM") open for public comment until July 3, 2024. CISA specifically sought input on the following:

- Definitions of key statutory terms whose meaning CIRCIA left to CISA rulemaking, including what constitutes a "covered entity" and a "covered cyber incident."
- The form, manner, content, and procedures for submission of reports required by CIRCIA.
- Areas where obligations under CIRCIA may duplicate or conflict with existing cyber reporting obligations.
- Policies and procedures, such as enforcement procedures and information protection policies, that will be required to implement CIRCIA.

CIRCIA requires the Director of CISA to publish the Final Rule within 18 months of the proposed rules, or by no later than September 2025.

In addition to the CISA rulemaking, the US Securities and Exchange Commission (SEC) on July 26, 2023 adopted rules increasing existing cybersecurity requirements, requiring publicly

[10] DEPARTMENT OF HOMELAND SECURITY [Docket ID: CISA–2022–0010] Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Available at https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022

listed companies to report to the SEC cybersecurity incidents, their cybersecurity capabilities, and their board's cybersecurity expertise and oversight.[11] The SEC rules address cyber attack reporting by requiring current reporting about material cybersecurity incidents on Form 8-K. They also address the same issues behind cybersecurity self-certification by requiring periodic disclosures regarding, among other things:

- A registrant's policies and procedures to identify and manage cybersecurity risks.
- Management's role in implementing cybersecurity policies and procedures.
- Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk.

Despite the recission of other cybersecurity rules at the SEC under the current presidential administration, this rule remains in force.

The communications sector is also subject to a host of other existing reporting requirements at the federal level, such as the FCC's Disaster Information Reporting System (DIRS), Network Outage Reporting System (NORS), and CPNI breach notification portal. Many communications providers also have reporting obligations as government contractors under the Defense Federal Acquisition Regulation Supplement (DFARS) clause, DFARS 252.204-7012(c), and/or other federal regulatory or contract regimes such as conditions associated with transactions reviewed under the Committee on Foreign Investment in the United States (CFIUS). The sector also has long-established, voluntary cyber incident reporting relationships with the FBI and the Secret Service. Publicly traded communications providers are also subject to existing SEC requirements to disclose cyber incidents, as discussed above.

---

[11] SECURITIES AND EXCHANGE COMMISSION 17 CFR Parts 229, 232, 239, 240, and 249 [Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22] RIN 3235-AM89 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (available at https://www.sec.gov/news/press-release/2022-39).

In addition, the FCC issued a Declaratory Ruling and Notice of Proposed Rulemaking on January 16, 2024 seeking comments on "ways to strengthen the cybersecurity posture of our nation's communications systems and services" and proposing to require covered communications service providers to submit an annual certification attesting that they have created, updated, and implemented cybersecurity and supply chain risk management plans.[12] The NPRM portion of this order is on hold pending review by the FCC Chairman or his designee, based on a January 20, 2025 executive order.[13]

Because of the plethora of federal regulatory obligations associated with critical infrastructure providers, Congress directed the Department of Homeland Security to convene the Cyber Incident Reporting Council (CIRC), which is tasked with reducing the burden on industry by reviewing, deconflicting, and harmonizing federal cyber incident reporting requirements.[14] The CIRC's final report was issued in September 2023.[15] The report determined that there are 45 different Federal cyber incident reporting requirements created by statute or regulation currently in effect. These 45 reporting requirements are administered by 22 different Federal agencies. The report acknowledged that this only includes federal requirements, not the wide variety of state, local, or international requirements to which entities are also subject.

---

12 https://docs.fcc.gov/public/attachments/FCC-25-9A1.pdf

13 https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/

14 https://www.dhs.gov/news/2022/07/25/readout-inaugural-cyber-incident-reporting-council-meeting

15 https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government

II. Verizon Response to Appendix A Questions

In this section Verizon provides its response to the specific questions listed in Appendix A to the Supplemental ANOPR. Verizon also incorporates its responses to the questions on the original ANOPR.

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 80053, and/or NIST Special Publication 80082?**

The Commission should not revise its existing rules until the CISA rulemaking is completed. At that point, the Commission should consider whether the new CISA rules, together with the other extensive federal level cybersecurity rules and requirements, obviate the need for state-specific requirements, either generally or for the communications industry specifically. If state-specific rules are still determined to be necessary, then Verizon supports the self-certification concept, which is the current structure of the Commission's rules, rather than the more onerous potential frameworks discussed in the original NPRM. The Staff Working Proposals at Appendix B to the Supplemental ANOPR follow a self-certification model.

Once the federal rules are finalized, and if state rules are still necessary, then the Commission can determine whether self-certification to federal or industry standards would be workable, at least for entities that are subject to federal standards.[14] Verizon's enterprise-wide Information Security Policy is aligned with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework 2.0. One would expect these NIST standards to be updated from time to time, so that any regulatory requirements for self-certification should be flexible enough to accommodate updated standards and to recognize the different standards that might apply to various industries or companies.

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?**

The Commission should not revise its existing rules until the CISA rulemaking is completed. At that point the Commission should consider whether any state-specific rules are necessary for those industries or entities already covered by federal rules, and if so, how those rules could be crafted to eliminate duplicative requirements. One possible method of classification would be to consider whether and to what extent an industry or company is already subject to federal requirements, where the Commission could reasonably rely on a self-certification of federal compliance. The Commission could then focus on more specific requirements or certifications appropriate for those industries or entities, if any, that are not subject to federal requirements.

    b. **Should the Commission specify the criteria it would consider in a petition to waive such requirements?**

If the Commission determines to continue a self-certification requirement, then the answer to this question regarding the criteria for waiver would likely change based on how specific or granular the requirements for self-certification turn out to be. The language in section 103.4 of the Staff Working Proposal seems reasonable in the context of Staff's proposal, although it should be modified to include the possibility of waiving section 103.2(d) for completeness.

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?

If the Commission determines to continue a self-certification requirement, it should craft its rule with enough flexibility so that self-certification to cybersecurity programs and plans that utilize equal or stricter standards and frameworks than those enumerated in the rule would automatically qualify rather than putting companies to the burden and expense of seeking a waiver.

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?

Verizon does not opine on whether smaller utilities would necessarily be less critical. While smaller utilities should not be required to certify to federal or industry standards and frameworks that do not apply to them, the absence of applicable federal or industry standards might be a factor that requires more Commission involvement in cybersecurity practices for smaller companies because all utility infrastructure can be critical in its own way.

e. How should the Commission account for changes and updates to those standards and frameworks over time?

If the Commission determines to continue a self-certification requirement, then it should word the rule to allow certification of compliance with federal law and/or industry standards including future changes. The Commission should await completion of the CISA rulemaking before proposing exact language.

f. How should the Commission confirm compliance with those requirements?

The Commission should not revise its existing rules until the CISA rulemaking is completed. As discussed in CISA's rulemaking order, CISA has investigatory and enforcement powers and the Commission should not duplicate compliance requirements that exist at the federal level.

g. How should the Commission enforce those requirements in the event of violations?

The Commission should defer to federal authorities, which can enforce compliance with federal requirements with regard to substance. For procedural issues, such as the failure to file a self-certification or other required report, the Commission can rely on its normal processes.

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).

The Commission should wait for the completion of the CISA rulemaking to consider specific permanent alterations to its rules. At that time, it should consider whether certifications or other filings required at the federal level would obviate the need for some or all entities to also file on the state level, or at a minimum would allow for a simpler, non-confidential certification form that simply affirms that all federal requirements have been met. Any approach that attempts to create a self-certification form that is public and not treated confidentially would have to ensure that it complies with this Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act. It would also have to be very careful not to require oversharing of information about cyber defenses that could give hackers an opportunity to leverage the disclosed information to compromise company networks.

Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act, 35 Pa. P.S. §§ 2141.1 et seq., prohibits an agency from disclosing "confidential security information," defined to include "[p]ortions of emergency response plans that are submitted to . . . the Pennsylvania Public Utility Commission or any other Federal, State or local agency dealing with response procedures or plans prepared to prevent or respond to emergency situations, except those portions intended for public disclosure, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures or specific security procedures" or "[a] security plan, security procedure or risk assessment prepared specifically for the purpose of preventing or for protection against sabotage or criminal or terrorist acts."

It may turn out that a "one-size-fits-all" solution is not appropriate for the self-certification process. Where certain companies or industry segments are already subject to robust review of their cybersecurity fitness by other agencies (such as CISA, the FCC, or the SEC), then the costs of duplicative submissions to this Commission would outweigh any benefits and at most a simple, non-confidential form would be sufficient. But for smaller entities or industries that might not be subject to the same level of oversight, the Commission might take a larger role in certifying their cybersecurity fitness and or require information to be provided that is protected as Public Utility Confidential Security Information.

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?**

Verizon is hopeful that once the CISA rulemaking is completed, this Commission will determine that certifications or other filings required at the federal level obviate the need for Commission-regulated communications companies to also file on the state level, or at a minimum would allow for a simpler, non-confidential certification form. If it turns out to be

necessary for Public Utility Confidential Security Information to be filed with the Commission, however, then 35 P.S. § 2141.3 requires the following:

> **(d) PROTECTING CONFIDENTIAL SECURITY INFORMATION.—** An agency shall develop such protocols as may be necessary to protect public utility records or portions thereof that contain confidential security information from prohibited disclosure under section 5. Such protocols shall ensure that:
>
> **(1)** Each copy of a record or portion thereof containing confidential security information is clearly marked as confidential and not subject to the provisions of the Right-to-Know Law.
>
> **(2)** Each copy of a record or portion thereof containing confidential security information is kept on site in a secure location, separate from the general records relating to the public utility, where it is available for inspection by authorized individuals.
>
> **(3)** Only authorized individuals, as designated by the agency, may have access to records or copies thereof containing confidential security information.
>
> **(4)** Authorized individuals, as designated by the agency, shall undergo training and sign an access agreement which summarizes responsibilities and personal liabilities if confidential security information is knowingly or recklessly released, published or otherwise disclosed.
>
> **(5)** A document tracking system is established to allow for records or copies thereof containing confidential security information to be traceable at all times to a single person.

The Commission has regulations governing the filing and handling of Public Utility Confidential Security Information. 52 Pa. Code § 102.3. The Commission should work within the scope of its regulations on this issue and if any changes to the handling of this information are found to be necessary, then they should be made in the context of changing that regulation for all Public Utility Confidential Security Information. Notably, the rule states that "[t]he Commission does not authorize the use of e-mail or any other electronic mail system to transmit records containing confidential security information." 52 Pa. Code § 102.3(g).

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?**

The legislative purpose articulated by CISA in its NOPR is broader than this Commission's statutory role with respect to the utilities it regulates. However, achievement of CISA's goals would necessarily also ensure that companies subject to its rules are providing reasonably adequate, reliable, continuous, and safe service to the public.

According to CISA, "CIRCIA's legislative history indicates that the primary purpose of CIRCIA is to help preserve national security, economic security, and public health and safety." It further notes that "[b]oth CIRCIA's legislative history and statutory text highlight a number of more discrete purposes within the broader goals of enhancing national and economic security, and public health and safety," such as:

- "trend and threat analysis,"
- "vulnerability and mitigation assessment,"
- "the provision of early warnings,"
- "incident response and mitigation,"
- "supporting Federal efforts to disrupt threat actors," and
- "advancing cyber resiliency."

CISA NPRM Section III.C.

While this Commission does not have an explicit statutory role corresponding to CIRCIA's goals of helping preserve national and economic security, the Commission's statutory role is sufficiently similar to CIRCIA's goal of protecting the public health and safety. The prevention or swift mitigation of cyber-security incidents will advance CIRCIA's purposes and this Commission's statutory mission.

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)).**

This is an area to be addressed by federal authorities, including CISA, and does not require action by this Commission.

    b. **Vulnerability and mitigation assessment (i.e., the identification of cyber vulnerabilities and the assessment of countermeasures that might be available to address them).**

This is an area to be addressed by federal authorities, including CISA, and does not require action by this Commission.

    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).**

This is an area to be addressed by federal authorities, including CISA, and does not require action by this Commission.

    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).**

This is an area to be addressed by federal authorities, including CISA, and does not require action by this Commission.

    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).**

This is an area to be addressed by federal authorities, including CISA, and does not require action by this Commission.

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?

This is an area to be addressed by federal authorities, including CISA, and does not require action by this Commission. However, should the Commission become aware of specific cybersecurity threat information of this nature it should share it with the parties at risk.

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

Verizon responds to this question in the context of the communications industry and does not address whether any other type of public utility or industry should be exempt from cyber incident reporting. Communications companies regulated by this Commission should be exempt from any new requirement to report cyber incidents. Not only does Chapter 30 of the Public Utility Code limit the Commission's authority to impose new reporting requirements on communications companies, but also there is sufficient oversight at the federal level with respect to the communications industry, including the ongoing CISA rulemaking on federal reporting requirements, so that state reporting requirements are not necessary. With respect to the Staff Working Proposals set forth in Appendix B to the Supplemental NOPR, a "telecommunications utility" (as defined in proposed section 103.1) should be exempt from the new reporting required by proposed Chapter 104.

Currently, communications providers are not subject to specific cyber incident reporting rules under the Commission's regulations. Verizon and other regulated telecommunications providers are and would continue to be subject to this Commission's rule at 52 Pa. Code § 67.1, which requires reporting of certain unscheduled service interruptions and allows "telephone utilities" to "file a comparable outage report required by the Federal Communications Commission" in lieu of certain information required by the rule. When the Commission revised

Section 67.1 in 2011, it recognized that the limitations in Chapter 30 of the Public Utility Code precluded it from adding new reporting requirements for telephone providers.[16] Notably, this was the same rulemaking in which the Commission added explicit cyber attack reporting rules for other industries, but it did not add them for telecommunications companies. This was the right decision at that time, and continues to be the right decision today.[17]

The statutory provision at 66 Pa. C.S. § 3015(e) specifically limits the reports the Commission is authorized to require from a local exchange telecommunications company.[18] A cyber attack report is not one of the reports that the legislature enumerated.[19] The Commission's authority to require ***any*** additional reporting from telephone carriers beyond the reports specifically enumerated in the statute is strictly limited by Section 3015(f)(1), which makes clear that "no report, statement, filing or other document or information, except as specified in subsection (e), shall be required" unless the Commission first makes specific written findings that the report is necessary to ensure that the company "is charging rates that are in compliance with this chapter and its effective alternative form of regulation" and that "the benefits of the

---

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

17 More recently, the Commission also recognized Chapter 30's restriction on new reporting obligations in its Diversity Reporting rulemaking. *Diversity Reporting of Major Jurisdictional Utilities*, Docket No. L-2020-3017284, Final Rulemaking Order entered April 14, 2022 at 7 ("With respect to Verizon's position that the Public Utility Code precludes any additional reports from local exchange telecommunications companies (LETCs), the PUC is constrained to agree.")

18 Verizon Pennsylvania LLC and Verizon North LLC are "local exchange telecommunications companies" operating under alternative regulation as defined in Chapter 30.

19 The only reports the Commission is authorized by law to require are: a network modernization plan report under section 3014(f); an annual financial report; an annual deaf, speech-impaired and hearing-impaired relay information report; an annual service report; universal service reports; an annual access line report; an annual statement of gross intrastate operating revenues; an annual state tax adjustment computation; and a bona fide retail request report under section 3014(c)(9). 66 Pa. C.S. § 3015(e).

report substantially outweigh the attendant expense and administrative time and effort required . . . to prepare it." 66 Pa. C.S. § 3015(f)(1).[20] Chapter 30 also directs the Commission to reduce regulation of telecommunications providers under its jurisdiction to "take into consideration the emergence of new industry participants, technological advancements, service standards and consumer demand,"[21] consistent with the stated legislative intent to "[r]ecognize that the regulatory obligations imposed upon the incumbent local exchange telecommunications companies should be reduced to levels more consistent with those imposed upon competing alternative service providers."[22] Competing alternative service providers are not and cannot be subjected to this type of state level reporting requirement as the Commission lacks the authority to require reporting from the large array of unregulated cable, wireless, and VoIP providers that compete directly with the regulated local exchange telecommunications companies.

Not only are new reporting requirements restricted by Chapter 30, but they are not necessary for the communications sector, which is already subject to reporting and other requirements from various federal agencies, as discussed in the Background section of these supplemental comments. State-specific reporting requirements that overlap federal rules can be counter-productive by diverting resources of covered entities away from incident mitigation. When cybersecurity professionals must devote time and attention to making difficult determinations about whether various different reporting requirements have been triggered, time

---

[20] In a previous Commission proceeding various parties, including two of the state legislators instrumental in the drafting of these provisions of Chapter 30, explained that both conditions must be satisfied in order for the Commission to require additional reporting, and that the test is not "either, or." The Commission did not decide the issue. *Section 3015(F) Review Regarding The Lifeline Tracking Report, Accident Report And Service Outage Report*, Docket No. M-00051900, 2005 Pa. PUC LEXIS 39 (Opinion and Order entered December 30, 2005).

[21] 66 Pa. C.S § 3019(b)(2).

[22] 66 Pa. C.S § 3011(13).

is taken away from responding to the incident itself. This is particularly so in the early stages of an incident when their expertise is needed to mitigate and investigate.

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?**

For the reasons discussed above, the Commission should not require cyber incident reporting from communications providers. The Commission's rule at 52 Pa. Code § 67.1 allows "telephone utilities" to "file a comparable outage report required by the Federal Communications Commission" in lieu of certain information required by the rule. Beyond that existing rule, however, Chapter 30 precludes a new reporting requirement requiring the submission of other information or documents provided to federal agencies. Moreover, the federal agencies will take any action that is necessary in response to federal reporting and any involvement by this Commission with the same reports would be duplicative.

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?**

The regulatory duplication or overlap would occur if the Commission were to require reporting of the same information that is required to be reported to federal authorities, or to require submission of copies of federal reports. At least with regard to the communications industry, the Commission should rely on the federal process and should not require state-specific reporting for the reasons discussed above.

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?**

The Commission could avoid regulatory duplication or overlap by permitting companies to certify their compliance with federal rules without additional state requirements.

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.

As Verizon reads the staff proposal, the physical security, emergency response, and/or business continuity aspects of the rule would continue to apply.

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.

The Commission should wait for the completion of the CISA rulemaking to consider specific permanent alterations to its rules. At that time, it should consider whether certifications or other filings required at the federal level would obviate the need for some or all entities to also file on the state level, or at a minimum would allow for a simpler, non-confidential self-certification form that affirms that all federal requirements have been met. The Commission should not add new cyber attack reporting requirements for the communications industry, for the reasons discussed above. These guidelines will allow the Commission to minimize the costs of any regulatory changes and avoid duplication and overlap with federal requirements.

At the appropriate time the Commission should consider the costs and benefits of any rules it seeks to adopt. Section V of the CISA NOPR contains an extensive discussion and analysis of the potential costs of CISA's proposed rules, which perhaps could provide a resource to the Commission. As to benefits, to the extent the Commission adopts requirements that overlap with or duplicate federal requirements there would be little or no benefit from additional regulatory burdens.

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.

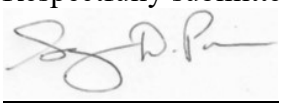
Verizon refers the Commission to the discussion in Sections I (Background) of these comments explaining how the nature of the communications industry means that network resiliency and data integrity must be a key business and operational priority and that Verizon and the communications sector have a long history of protecting against threats to customers' security and ensuring the reliability and resilience of communications services against all manner of hazards, including cyber threats. It details how Verizon is a leader in industry cyber security initiatives and also its extensive federal regulatory and law enforcement involvement in cybersecurity issues. Verizon also refers the Commission to its discussion of Chapter 30's limitation of new reporting requirements on local exchange telecommunications companies, which precludes the imposition of new cyber attack reporting regulations on that segment.

III. Conclusion

Verizon appreciates the opportunity to provide supplemental comments on this important issue and stands ready to participate in further proceedings as the Commission directs.

Dated: July 16, 2025

Respectfully submitted,



Suzan D. Paiva (Atty No. 53853)
Verizon
900 Race St., 6th Floor
Philadelphia, PA 19107
(267) 768-6184
Suzan.d.paiva@verizon.com

Attorney for the Verizon Companies