900 Race Street
6th Floor
Philadelphia, PA 19107

Suzan DeBusk Paiva
Associate General Counsel
Suzan.d.paiva@verizon.com

February 8, 2023

VIA ELECTRONIC FILING
Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor
Harrisburg, PA 17120

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

Dear Secretary Chiavetta:

Enclosed please find Verizon's Comments regarding the November 10, 2022 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/sau

Suzan D. Paiva

SDP/sau
Enclosure

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 COMMENTS

On November 10, 2022, the Commission issued an Advance Notice of Proposed Rulemaking Order (ANOPR) seeking comments on potentially updating its regulations relating to cybersecurity self-certification and cyber attack reporting. In response to the December 10, 2022 publication of this ANOPR in the Pennsylvania Bulletin, Verizon[1] submits the following comments in which we explain that the Commission should await the completion of the ongoing rulemaking of the Cybersecurity and Infrastructure Security Agency (CISA), setting federal rules for cyber incident reporting and related issues, before considering changes to or elimination of its own state rules.

I. Introduction

Cybersecurity is one of the most important issues facing businesses today, and is key for telecommunications companies like Verizon that operate national and global broadband and communication networks. But now is not the time for the Commission to open a rulemaking to change its regulations in this area because significant proceedings are ongoing at the federal level, the results of which will inform this Commission's review of its own rules. The Commission should, at a minimum, await the outcome of CISA's[2] federal rulemaking that will

---

[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.

craft federal rules implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (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 and provides a deadline for it to do so.

As discussed in more detail in Section III of these Comments (Verizon's response to the Commission's specific questions), Verizon anticipates continuing to comply with Chapter 101 (self-certification for cybersecurity and other issues) and Chapter 67 (service outage reporting) while the federal CISA rulemaking is being completed. Verizon is not currently subject to specific Commission cyber attack reporting regulations (and, as discussed in more detail in Section III, Chapter 30 of the Public Utility Code precludes new cyber attack reporting requirements), but Verizon is a leader in cyber security initiatives on a company and industry basis and is subject to oversight from various federal agencies and law enforcement on this issue. It is crucial to our ability to serve our consumers that we lead in these initiatives, and that is a key reason why we do.

After the CISA rules have been issued, the Commission could refresh its request for comments to determine if it is still necessary to have state-specific cybersecurity and cyber attack reporting rules at all, and, if so, which entities should be covered and what terms should be used.

II. Background

A. Cybersecurity is 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 at this time, the Commission should be assured that protecting the security of our systems and networks is a top priority for Verizon.

To more effectively address the cybersecurity threats posed today, Verizon has a dedicated Chief Information Security Officer 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 Chief Information Security Officer 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) Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). As part of this policy, we have 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. We also publish 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]

[3] The 2022 Verizon Data Breach Investigations Report is available here: https://www.verizon.com/business/resources/reports/dbir/2022/introduction/

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-chairs the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC). Multiple Verizon subject matter experts are actively engaged in the CSRIC's working groups that are underway developing and publishing key security recommendations for 5G signaling protocols, Open Radio Access Network, software and cloud service supply chain, 911 over Wi-Fi, Wireless Emergency Alerts and 5G virtualization technology.[5]

- 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

---

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

5 https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-1

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

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

developing a Hardware Bill of Materials framework so purchasers of communications equipment can effectively and efficiently assess and manage supply chain risks.[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]

- Verizon was a founding member and is an active participant in the Council to Secure the Digital Economy (CSDE), which brings together multinational companies from across the communications and technology sectors to combat increasingly sophisticated and emerging cyber threats through collaborative actions. The CSDE leverages the expertise of members that represent major stakeholders in the global digital ecosystem. CSDE's International Botnet and IoT Security Guide is among the world's leading initiatives to dramatically reduce destructive botnet attacks. Since 2018, CSDE has brought together communications and technology sector leadership on an annual basis to identify practices and capabilities for combating threats related to botnets, such as malware propagation, denial-of-service attacks and the spread of corrosive disinformation.

- Verizon's President of Global Networks and Technology was recently appointed to the President's National Security Telecommunications Advisory Committee (NSTAC), which advises the White House on the reliability, security, and preparedness of vital communications and information infrastructure. Verizon was chosen as an industry member of NSTAC to provide national security and emergency preparedness solutions by providing innovative policy recommendations backed by an industry perspective.[10]

---

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

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

10 https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/03/president-biden-announces-appointments-to-national-security-telecommunications-advisory-committee/

B. There is 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 is participating 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. On September 12, 2022, CISA issued a request for information (RFI) seeking input from stakeholders in preparation for issuing proposed rules.[11] While commenters can provide input on any aspect of CIRCIA, CISA is specifically seeking 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 proposed rules in the form of a Notice of Proposed Rulemaking (NPRM) within 24 months of CIRCIA's enactment, or by no later than March 2024**.** A Final Rule must be published within 18 months of the proposed rules, or by no later than September 2025**.**

[11] 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

In addition to the CISA rulemaking, the US Securities and Exchange Commission (SEC) in March of 2022 proposed rules increasing existing cybersecurity requirements, which would require publicly listed companies to report to the SEC cybersecurity incidents, their cybersecurity capabilities and their board's cybersecurity expertise and oversight.[12] These proposed SEC rules would increase and standardize disclosures regarding cybersecurity risk management, strategy, governance and incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. If enacted as proposed, these rules also are likely to have some duplication with this Commission's rules. They would address cyber attack reporting by requiring current reporting about material cybersecurity incidents on Form 8-K. They would 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.
- Updates about previously reported material cybersecurity incidents.

Extensive public comments have been filed with the SEC questioning, for example, whether the proposed rules strike the correct balance between the costs and benefits of reporting, including the timing; if it would be better to allow incidents to be kept confidential so as not to interfere in investigation and resolution of the incident; and whether there is duplication with other reporting requirements. The matter remains open before the agency.

---

[12] 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)

The communications sector is 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 requirement to disclose cyber incidents. Indeed, because of the plethora of federal regulatory obligations associated with critical infrastructure providers, Congress directed the Department of Homeland Security to convent 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.[13]

III. Response to specific Commission topics

In this section Verizon provides its response to the specific topics listed in Appendix A to the ANOPR.

A. Cybersecurity Self-Certification

1. Updating Terms and Concepts (ANOPR Appendix A, ¶ 2)

As discussed above, Verizon suggests that the Commission postpone any official rulemaking to update its cybersecurity self-certification regulations until after CISA publishes its final regulations implementing CIRCIA. The federal statute requires CISA to publish proposed rules

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

within 24 months of CIRCIA's enactment, or by no later than March 2024, and publish its final rules within 18 months of the proposed rules, or by no later than September 2025. At that point this Commission will be in a better position to determine what, if any, state cybersecurity self-certification regulations are still necessary in consideration of the costs and benefits of state-specific requirements and the avoidance of duplication with federal rules. If the Commission determines that state regulations are still needed, then it can consider which entities should be covered and conform relevant terms and concepts to the CISA regulations for the sake of uniformity. It can also consider whether certification of compliance with federal standards is sufficient for some or all entities.

In the interim, Verizon expects to continue to comply with the Commission's existing cybersecurity self-certification process in Chapter 101 while the CISA rulemaking proceeds. If the comments in response to this ANOPR reveal that the existing process is causing an undue hardship to smaller entities and/or that the costs of their compliance outweigh the benefits, then the Commission could consider a temporary waiver for those entities. 52 Pa. Code § 5.43.

2. Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities (ANOPR Appendix A, ¶s 3-7)

As discussed above, the Commission should not revise its existing rules until the CISA rulemaking is completed. In response to paragraphs 3 through 5 of the ANOPR Appendix A, however, if state-specific self-certification rules are still determined to be necessary after the CISA rulemaking is completed, then one of the first two bullet points on page 12 would be the better approach (self-certification to PUC criteria or self-certification to federal and/or industry standards). Once the federal rules are finalized, we hope that self-certification to those federal standards would be workable, at least for entities that are subject to federal standards.[14]

[14] A self-certification approach would allow the Commission also to continue to require self-certifications of physical security, emergency response and/or business continuity if that is determined to be necessary in light of federal requirements.

The other proposed approaches (third-party certification, onsite review or mandatory submission of documents) suffer from a number of flaws. First, these requirements would be unnecessarily burdensome, both for the utilities to provide and for the Commission staff to review, and possibly duplicative where most or all of these companies will be subject to reporting on these issues at the federal level through CISA, the SEC, the FCC and/or law enforcement. Second, it is very likely that the information required would be confidential under the Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act, 35 Pa. P.S. §§ 2141.1, et seq., (discussed below), thereby increasing the burden and complexity for Commission staff of storing and reviewing the information. Similarly, the more detailed the information required to be handled and stored by the Commission, the more it increases the risk of bad actors obtaining access to it improperly and using it to assist in carrying out cyber attacks. Finally, with regard to telecommunications companies, requiring the submission of new information that is not required by the current rules risks running afoul of Chapter 30's limitation on new reporting requirements (discussed below).

In response to paragraphs 6 and 7 of Appendix A, to the extent there are entities regulated by the Commission that are not subject to Chapter 101's cybersecurity self-certification requirements, the Commission should monitor whether these entities become subject to the CISA and/or SEC regulations before it makes a determination of the necessity of bringing them under state regulation. If information regarding the cybersecurity fitness, physical security, emergency response and/or business continuity plans of these entities is needed in the interim, the Commission has authority under 66 Pa.C.S. § 504 to request information. After the CISA regulations are final, it might be appropriate to exempt certain entities from this Commission's process permanently, or even to eliminate the cybersecurity self-certification altogether.

3. Improving the Self-Certification Form (SCF) Process (ANOPR Appendix A, ¶s 8-9)

Chapter 101 provides that "[a] Self Certification Form filed at the Commission is not a public document or record and is deemed confidential and proprietary." 52 Pa. Code § 101.5. Likely this was intended to ensure compliance with Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act, 35 Pa. P.S. §§ 2141.1 et seq., which 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." The ANOPR notes the complexities for Commission staff from handling these forms as confidential information, as well as the fact that different industries are required to file their forms at different times.

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 Pennsylvania law. 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.

The Commission 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." ANOPR at 15-16. Verizon supports the concept of reducing company and staff administrative burdens. But 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. 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. 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.

B. Cyberattack Reporting

1. Updating Cyber Attack Reporting Regulations (ANOPR Appendix A, ¶s 10-11)

For this section, Verizon limits its comments to the issue of whether the Commission should update its cyber attack reporting regulations to include telecommunications carriers. It should not. Not only does Chapter 30 of the Public Utility Code limit the Commission's authority to impose new reporting requirements, but there is sufficient oversight at the federal level with respect to the telecommunications industry so that state reporting requirements are not necessary.

The ANOPR notes that communications providers are not subject to specific cyber attack reporting rules under the Commission's current regulations. However, Verizon and other regulated telecommunications providers are subject to this Commission's rule at 52 Pa. Code

67.1, which requires reporting of certain service outages 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 certain types of telephone providers.[15] 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. More recently, the Commission also recognized Chapter 30's restriction on new reporting obligations in its Diversity Reporting rulemaking.[16]

The answer is the same with respect to the consideration of new cyber attack reporting regulations now. 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.[17] A cyber attack report is not one of the reports that the legislature enumerated.[18] The Commission's authority to require ***any*** additional reporting from telephone carriers beyond the

---

15 *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.")

16 *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.")

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

18 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).

specifically enumerated reports is strictly limited as Section 3015(f)(1) 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 report substantially outweigh the attendant expense and administrative time and effort required . . . to prepare it." 66 Pa. C.S. § 3015(f)(1).[19] 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,"[20] 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."[21] The Commission clearly lacks the authority to require cyber attack reporting from the large array of unregulated cable, wireless and VoIP providers that compete directly with the regulated local exchange telecommunications companies.[22]

---

[19] 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).

[20] 66 Pa. C.S § 3019(b)(2).

[21] 66 Pa. C.S § 3011(13).

[22] Not only is this proof required by 66 Pa. C.S. § 3015(f)(1) before a new reporting requirement could be imposed on Verizon, but a similar analysis is also required by the Regulatory Review Act generally. The purpose of the regulatory review process is to avoid "regulations being promulgated without undergoing effective review concerning cost benefits, duplication, inflationary impact and conformity to legislative intent," and therefore the Regulatory Review Act requires an executive agency "to justify its exercise of the authority to regulate before imposing hidden costs upon the economy of Pennsylvania." 71 P.S. § 745.2. The Regulatory Review Act requires a showing that the proposed regulations are in the public interest. This proof requires evidence of the "[e]conomic or fiscal impacts of the regulation," such as "[d]irect and indirect costs to . . . the private sector," "[a]dverse effects on productivity or competition," the costs of preparing "required reports,

As discussed in Section II (Background), the communications sector is subject to reporting and other requirements from various federal agencies and so no state-specific cyber attack reporting requirement for regulated communications companies is needed. 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 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.

2. Merging the Self-Certification and Cyber Attack Reporting Regulations (ANOPR Appendix A, ¶12)

The Commission 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. In principle, simplification and uniformity of regulatory requirements is a worthwhile consideration. But the Commission should recognize the justified reasons why certain industry segments may be subject to different reporting or certification requirements. For example, there may be legal limitations on reporting requirements, such as the restriction on new reporting requirements for local exchange telecommunications companies under 66 Pa. C.S. § 3015. There may be different considerations of duplications and costs versus benefits if some industry segments are subject to different or more robust requirements at the federal level. There may be differences based on company size, public trading status and industry vulnerabilities. In any event, the Commission

forms or other paperwork," the "[n]eed for the regulation," and the "[r]easonableness of requirements." 71 P.S. § 745.5b(b).

will be in a better position to evaluate these issues if it waits for the outcome of the CISA rulemaking.

3. Cost-Benefit Analysis (ANOPR Appendix A, ¶ 13)

The Commission seeks comment on how the costs and benefits associated with its existing regulations, and any revisions thereto, can be objectively quantified and evaluated. It is premature to conduct a cost versus benefits analysis at this time because the Commission does not yet know what the CISA regulations will require and what industries or entities will be subject to them. Speaking generally, a cost benefit analysis should consider whether the same status or events are subject to other reporting requirements, particularly at the federal level, not only with the CISA regulations but also with FCC, FTC, SEC and/or law enforcement requirements. If federal reporting is already required, then duplicative reporting burdens at the state level have little or no benefit. This is important because resources should not unnecessarily be diverted away from incident mitigation by requiring cybersecurity professionals to devote time and attention to determining whether various reporting requirements have been triggered and to preparing duplicative reports. A self-certification that the company complies with federal requirements may be sufficient in this instance. A cost benefit analysis should also consider if the format of the reports themselves could give hackers a roadmap to leverage the disclosed information to compromise company networks, particularly if they are not filed confidentially, in which case the cost of the reporting requirement would be heavy and outweigh any benefits.

4. Eliminating Regulatory Duplication and Overlap (ANOPR Appendix A, ¶14)

The Commission seeks comment on the potential for conflict, overlap, redundancy, or other bases warranting review in the interplay between the its own cybersecurity regulations (and revisions thereto) and federal initiatives. Verizon agrees that this is an important consideration,

but any permanent changes to the Commission's rules should await the outcome of the CISA rulemaking so that the extent and details of these federal requirements can be known.

5. Other Matters (ANOPR Appendix A, ¶ 15)

The Commission finally 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." Verizon refers the Commission to the discussion in Sections I (Introduction) and II (Background) of these comments. In those sections, Verizon explains 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 Section III(B)(1) of these comments, discussing 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.

IV. Conclusion

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

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

Dated: February 8, 2023