Before the
Pennsylvania Public Utility Commission
Harrisburg, PA 17105-3265

In the Matter of	**)**	
	)	
Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting	**)** **)** **)**	L-2022-3034353

COMMENTS OF THE BROADBAND COMMUNICATIONS ASSOCIATION OF PENNSYLVANIA

The Broadband Communications Association of Pennsylvania ("BCAP")[1/] submits these comments on behalf of its members in response to the Commission's Advance Notice of Proposed Rulemaking Order ("ANOPR") in the above-captioned proceeding.[2/] The AONPR seeks comment on the sufficiency of the Commission's existing cybersecurity regulations to address the current and future cybersecurity threat landscapes.[3/]

INTRODUCTION AND SUMMARY

Cybersecurity plays a significant role in the overall success of the communications sector. The cable industry, which includes the Commonwealth's leading broadband providers, and the communications sector as a whole continue to be committed to network security. Pennsylvania's cable companies work every day to detect, prevent, and mitigate cybersecurity threats of all forms – including threats to secure internet routing – to minimize their impact on

[1/] BCAP is an association of Pennsylvania cable operators, equipment suppliers, programmers, and other allied companies. It advocates, communicates, and educates about industry positions to public policy makers, opinion leaders, and the general public in order to enhance member companies operations, competitiveness and profitability.

[2/] *See Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting*, Pa. Pub. Util. Comm'n, No. L-2022-3034353, Advance Notice of Proposed Rulemaking Order (rel. Nov. 10, 2022) ("*ANOPR*").

[3/] *See ANOPR* at 2.

broadband networks and consumers. The cable industry has a long history of providing its customers with the benefits of a secure network, including through its participation in, and support for, the development and implementation of key cybersecurity best practices and technical standards. BCAP and its members therefore support the Commission's efforts to ensure that its regulations adequately address the current and future cybersecurity threat landscapes.

As detailed more fully below, the Commission should delay adoption of any new or revised cyber attack reporting rules until the pending proceeding by the Cybersecurity and Infrastructure Security Agency ("CISA") to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") is complete. BCAP also urges the Commission to ensure that any new or revised cybersecurity certification or planning rules in Pennsylvania reflect the success of voluntary, public-private partnership efforts such as the Cybersecurity Framework developed by the National Institute of Standards and Technology ("NIST"). In addition, any new or revised rules should reflect the communications sector's strong current cybersecurity practices, while also acknowledging that the Commission's jurisdiction for cybersecurity oversight does not extend to cable and broadband and other non-telecommunications services.

I. THE COMMUNICATIONS INDUSTRY HAS INVESTED AND ENGAGED IN ROBUST AND EFFECTIVE CYBERSECURITY MEASURES

A. The Communications Industry Has Strong Incentives to Maintain Responsible Cyber Defense Measures

Ensuring network safety and security via strong cybersecurity practices is a paramount responsibility of any broadband network provider. The business success of any internet service provider is tied directly to maximizing customers' network usage and trust – both of which hinge on providing a safe, trusted, and secure network environment. As an association representing more than a dozen cable providers that offer broadband, video, and voice services to over three million residential and business broadband customers throughout the Commonwealth, ensuring the safety and security of networks is one of BCAP members' top priorities.

BCAP members' customers depend on our companies' network infrastructure to engage in commerce, access entertainment content, and conduct an increasingly wide range of activities and transactions throughout the Commonwealth. So our members' business success depends upon deterring, detecting, and responding to cybersecurity threats and vulnerabilities. BCAP members protect their customers from malicious activity and cyber threats by utilizing some of the most advanced tools, strategies, and protocols available today for preventing and addressing cybersecurity attacks.

B. The Communications Industry Continues to Make Substantial Investment in Cybersecurity Tools, Capabilities, and Protocols

In the Commonwealth alone, cable companies have invested over $10 billion of private capital in network infrastructure to build some of the nation's largest and most robust broadband networks and services.[4/] To ensure the safety and security of this infrastructure – and encourage its use by Pennsylvania residents – the cable industry also has invested heavily in cybersecurity – and continues to do so each year.

The cable industry has strong incentives to take seriously external threats to network security and focus its investments on technologies that are safe, secure, and reliable. Comcast, for example, has made traditional investments in network, endpoint, application, infrastructure, and data security infrastructure and tools. It has established and managed a mature, 24x7, geo-distributed, cybersecurity operations center that provides it with broad visibility across the cyber

[4/] *See Broadband Cable Pennsylvania Impact*, BCAP, https://www.bcapa.com/issue-briefs-2/f (last visited Feb. 7, 2023). Nationally, cable companies' private capital investment exceeds $245 billion. *See Cable Today*, BCAP, https://www.bcapa.com/cable-today/ (last visited Feb. 7, 2023).

threat landscape.[5] Like many communications service providers, Comcast also employs a defense-in-depth strategy, with multiple layers of detection and prevention controls in place, and it has invested heavily in threat intelligence, with multiple partnerships in open source, government, and commercial inputs.[6] BCAP members also conduct targeted threat hunts, build tools to make security easy for development teams, assess third-party vendors, and employ robust security operations programs. The companies regularly implement cyber defense programs that rely upon building security into their products and services,[7] conforming to Zero-Trust principles, and using data science and machine learning to help with earlier detection and response.[8]

II. INDUSTRY-DRIVEN, VOLUNTARY MEASURES REMAIN THE MOST EFFECTIVE AND RESPONSIVE MEANS TO ADDRESS KEY CYBER ISSUES

Flexible standards forged via industry-driven best practices and initiatives have been the cornerstone of successful cyber policy efforts, such as the NIST Cybersecurity Framework.[9] The ANOPR itself recognizes the value and benefits of the Framework, noting that it "has led the

[5] *See Privacy Center*, XFINITY, https://www.xfinity.com/privacy (last visited Feb. 7, 2023) ("We help protect you with multiple layers of security that automatically detect and block hundreds of thousands of cyber events every second and a team of security experts who work to protect you 24 hours a day, 365 days a year.").

[6] *See ThreatQuotient Selected By Comcast To Support Cybersecurity Operations*, BUSINESS WIRE (May 17, 2022, 8:00 AM), https://www.businesswire.com/news/home/20220517005274/en/ThreatQuotient-Selected-By-Comcast-To-Support-Cybersecurity-Operations.

[7] *See, e.g.*, *Introducing eero Secure – Internet Security Made Simple*, BLUE RIDGE (June 2, 2021), https://www.brctv.com/blog/homefi-eero-secure-internet-security-made-simple ("But HomeFi is more than just an amazing mesh WiFi system. It's a tool that helps you . . . keep your devices protected against cyberthreats.").

[8] *See, e.g.*, *Network*, ARMSTRONG, https://armstrongonewire.com/Network (last visited Feb. 7, 2023) (noting that Armstrong has "invested in the latest security and network technology that automatically detects and blocks thousands of cyber security events each day.)

[9] *See Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("NIST Cybersecurity Framework").

way in the advancement of cybersecurity standards" and "provides a model and a process to increase cybersecurity maturity in any organization."[10/] The keys to the success of the NIST Cybersecurity Framework have been the collaborative and inclusive process employed by the government over the last decade and NIST's recognition that a flexible, voluntary framework would be the best means to strengthen the country's overall cyber defense posture. Conversely, prescriptive rules are ill-suited for bolstering cyber defenses because they are generally backward-looking and static in circumstances in which delivering security requires companies to be agile, flexible, and forward-looking.

In 2014,[11/] Congress codified the lead role played by NIST in formulating its *Framework for Improving Critical Infrastructure Cybersecurity*,[12/] which has become the seminal document on cybersecurity risk management for the private sector. Both the NIST Cybersecurity Framework and the codification of the NIST process via enactment of the Cybersecurity Enhancement Act of 2014 reflected and advanced the clear Congressional policy preference for reliance upon voluntary mechanisms and industry-driven initiatives to combat cybersecurity threats. The Act also established "voluntary, consensus-based, industry-led" measures as the preeminent Federal policy mechanism for strengthening the cyber defenses of American companies.[13/] Other Federal agencies, including the Department of Homeland Security ("DHS"), the Department of Commerce, and the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability ("CSRIC") have played key role in

[10/] *ANOPR* at 11.

[11/] *See* Cybersecurity Enhancement Act of 2014, P.L. No. 113-274, § 101(b) (as codified in 15 U.S.C. § 272(e)).

[12/] *See* NIST Cybersecurity Framework.

[13/] *See* P.L. No. 113-274., § 101(a) (as codified in 15 U.S.C. § 272(c)(15)).

advancing cybersecurity through voluntary measures and best practices in such areas as botnet prevention, supply chain risk management, critical infrastructure security, internet routing security, secure software development, and internet of things ("IoT") device standards.

The voluntary nature of the standards and practices developed through these initiatives to their adoption and use, providing companies with the flexibility and full discretion to tailor the recommended procedures and tools to best comport with their particular network assets, business operations, and corporate structure. NIST itself stressed the importance of the "voluntary" nature of the Cybersecurity Framework, noting that it is designed to use "business drivers to guide cybersecurity activities" and to "manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses."[14/] Any action taken by the Commission in this proceeding should build upon – and not depart from – the success of the approach taken by NIST and other Federal agencies that rely upon voluntary best practices and industry consensus standards.

III. THE COMMISSION'S APPROACH TO COMMUNICATIONS COMPANIES IN THIS PROCEEDING SHOULD REFLECT THE COMMUNICATIONS SECTOR'S STRONG CYBERSECURITY PRACTICES AND THE LIMITS OF THE COMMISSION'S JURISDICTION

U.S. national communications and data transit network operators have some of the most sophisticated and well-resourced security operations in the world. In addition to deploying robust security operations centers, industry best practices on cybersecurity, and leading edge cyber defense tools, communications companies also have considerable experience collaborating with key Federal and state agencies on cybersecurity to maintain secure, reliable connectivity. As noted above, the communications sector partners with DHS, the Department of Commerce,

[14/] NIST Cybersecurity Framework at v.

the FCC, the White House Office of the National Cyber Director, and other Federal government entities on a broad array of cybersecurity initiatives, ranging from securing critical infrastructure, cyber threat information sharing, bolstering defenses against botnet attacks, and addressing supply chain risks and vulnerabilities.[15/] At the state level, the communications sector participates in statewide cyber incident exercises with the Commission to practice responses to potential threats, and the Commission partners with the communications sector and other stakeholders to regularly monitor for cyber threats to critical information systems.[16/]

The communications sector has attained a relatively mature level of cybersecurity protection in part because its entire business model depends upon customers trusting the security of its networks. By contrast, some portions of utility sectors, such as water supply and treatment plants and power generation infrastructures, may be more vulnerable to cyber threats due to the integration of their information systems with their control technologies and the potential for resource limits to hinder deployment of up-to-date cyber defense tools and protocols that could better protect their business networks and industrial control systems.[17/]

[15/] *See, e.g.*, *Cyber Assessments*, CISA, https://www.cisa.gov/cyber-assessments (last visited Feb. 7, 2023); *Communications Security, Reliability, and Interoperability Council VIII*, FCC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-1 (last visited Feb. 7, 2023); *The Office of the National Cyber Director Requests Insight and Expertise on Cyber Workforce, Training, and Education: An RFI & Virtual Reverse Stakeholder Day Effort*, WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2022/10/ONCD-Workforce-and-Education-RFI.pdf (last visited Feb. 7, 2023).

[16/] *See* Press Release, *PUC Highlights Importance of Critical Utility Infrastructure*, PA. PUB. UTIL. COMM'N (Oct. 27, 2022), https://www.puc.pa.gov/press-release/2022/puc-highlights-importance-of-critical-utility-infrastructure.

[17/] *See, e.g.*, *Small Utilities Must Master Cybersecurity*, FORBES (Oct. 3, 2022, 3:22 PM), https://www.forbes.com/sites/tanium/2022/10/03/small-utilities-must-master-cybersecurity/?sh=5c518bf7aa01 ("[Small] utilities must often contend with technology that is too old for modern cyber tools, a persistent lack of trained cybersecurity professionals, and IT staff that must wear many hats."); Ryan Morrison, *Utility Companies Most at Risk of Cyberattack – Moody's*, TECHMONITOR (Sept. 20, 2022), https://techmonitor.ai/technology/cybersecurity/utility-companies-cyberattack (Moody's "found water companies were among the most at risk of any sector. While the financial reward for attacking a water or electricity company was relatively low, they often have minimal security measures in

These divergences among sectors underscore the drawbacks of one-size-fits-all prescriptive rule approaches. For example, the ANOPR notes that self-certification and cyber attack reporting regulations applicable to steam utilities originated as a result of a 2007 steam pipeline explosion and concerns about steam pipeline safety, which carry the potential for significant adverse public impact.[18/] Similar concerns arise concerning the potential risks to public health and safety from cyber attacks targeting operational technology governing electric, gas, and water utilities. By contrast, Pennsylvania cable companies, due to their ongoing investments in cybersecurity, have largely been spared from high-profile, broad-impact cyber attacks, and Federal officials have long recognized the capacity of communications networks to contain and mitigate the potential disruptive effects of such attacks.[19/]

The Commission should refrain from uniform approaches that would saddle the communications sector with obligations and directives that are not commensurate with the maturity of its cyber defense efforts. Such restraint also is appropriate because whatever cybersecurity oversight authority is afforded to the Commission by virtue of its jurisdiction over

place, making them attractive targets"); *Cybersecurity Threats to the US Water Industry*, TRIPWIRE (Sept. 13, 2022), https://www.tripwire.com/state-of-security/cybersecurity-threats-to-the-us-water-industry ("The fragmented nature of water utility coverage coupled with low budgets and limited technologic expertise means many systems are outdated and under-protected. . . . While cybersecurity challenges are present throughout the utility sector, the water industry is particularly vulnerable"); *Cybersecurity For Utilities: Municipal Utilities Have Become A Major Target*, BITLYFT (June 2, 2021), https://www.bitlyft.com/resources/cybersecurity-for-utilities; *Electricity Grid Cybersecurity – DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GOVERNMENT ACCOUNTABILITY OFFICE (Mar. 2021), https://www.gao.gov/assets/gao-21-81.pdf (noting particular vulnerabilities associated with older legacy electric grid industrial control systems). *See also ANOPR* at 16 (noting "convergence of IT and OT in the utility industry increases the risk of cyber threats arising in the IT environment threatening OT").

[18/] *See ANOPR* at 5.

[19/] *See, e.g.*, INTERNET ARCHITECTURE IS CONSIDERED RESILIENT, BUT FEDERAL AGENCIES CONTINUE TO ADDRESS RISKS, U.S. GOVERNMENT ACCOUNTABILITY OFFICE 12-13 (2022), https://www.gao.gov/assets/gao-22-104560.pdf.

public utilities would not extend to non-utility offerings, such as cable, broadband, VoIP, and other non-telecommunications provided by cable companies. Nor do such companies fall within the scope of rules applicable to "jurisdictional utilities."[20/]

IV. ANY NEW CYBER MEASURES TAKEN BY THE COMMISSION IN THIS PROCEEDING SHOULD PROMOTE UTILIZATION OF INDUSTRY-DRIVEN CONSENSUS BEST PRACTICES

The ANOPR states 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."[21/] These consist of: (i) requiring a public utility to self-certify that it has a plan,[22/] a program, or both, that complies with the criteria set forth in the Commission's regulations and to report annually to the Commission that such plans and/or programs exist and are updated and tested annually; (ii) requiring 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

[20/] *See ANOPR* at 3.

[21/] *See id.* at 12.

[22/] The existing cybersecurity and business continuity plan requirements in Section 101.3(a) of the Commission's rules applicable to jurisdictional utilities specify as follows:
(2) A cyber security plan must, at a minimum, include:
(i) Critical functions requiring automated processing.
(ii) Appropriate backup for application software and data. Appropriate backup may include having a separate distinct storage media for data or a different physical location for application software.
(iii) Alternative methods for meeting critical functional responsibilities in the absence of information technology capabilities.
(iv) A recognition of the critical time period for each information system before the utility could no longer continue to operate.
(3) A business continuity plan must, at a minimum, include:
(i) Guidance on the system restoration for emergencies, disasters and mobilization.
(ii) Establishment of a comprehensive process addressing business recovery, business resumption and contingency planning.
(4) An emergency response plan must, at a minimum, include:
(i) Identification and assessment of the problem.
(ii) Mitigation of the problem in a coordinated, timely and effective manner.
(iii) Notification of the appropriate emergency services and emergency preparedness support agencies and organizations.

Commission that such plans and/or programs exist and are updated and tested annually; (iii) requiring 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 Commission; (iv) integrating an onsite review of cybersecurity measures, plans, and programs into the Commission's public utility management audit process and examining cybersecurity measures, plans, and programs in place as a part of the management audit function; and (v) requiring a public utility to file a confidential copy of its cybersecurity plans and programs with the Commission and enabling the Commission to directly review and comment on the adequacy of such plans and programs and, where deficiencies exist, require conformance with regulatory standards.[23/]

The self-certification provisions in the existing rules set forth key plan elements that are integral to ensuring a baseline level of cybersecurity. The Commission need not revise the elements but could provide an alternative means of compliance by incorporating the second option enumerated above to specify that a jurisdictional utility could satisfy Section 101.3 via self-certification of compliance with a leading Federal or industry cybersecurity standards framework. This approach has worked effectively in other states, such as Ohio,[24/] Utah,[25/] and Connecticut,[26/] which have pegged compliance with cybersecurity rules to conformity with any of the following data security guidelines/best practices: (i) the NIST Cybersecurity Framework; (ii) NIST SP 800-171, which set forth recommended practices for protecting unclassified

[23/] *See ANOPR* at 12-13.

[24/] *See* Ohio Rev. Code Ann. § 1354.03 (Reasonably confirms to industry standard.).

[25/] *See* Utah Code Ann. § 78B-4-703 (Components of a cybersecurity program eligible for an affirmative defense.).

[26/] *See* Conn. Gen. Stat. § 42-901 (Adoption of cybersecurity controls by businesses. Exemption from punitive damages.).

information in non-Federal systems and organizations; (iii) NIST 800-53, which sets forth security and privacy controls for Federal information systems; (iv) the Security Assessment Framework for the Federal Risk and Authorization Management Program; (v) the Center for Internet Security Critical Security Controls for Effective Cyber Defense, also known as the SANS-20 critical security controls; or (vi) the ISO/IEC 27000-series cybersecurity standards and practices.

The Commission should refrain from adopting approaches predicated upon third-party certification, audit processes, or Commission review of the cybersecurity plans of jurisdictional utilities. Such approaches are in tension with one of the key drivers of adoption and utilization of the best practices and standards frameworks delineated above – flexibility to adapt and iterate cybersecurity plans to the recommended processes and standards for their particular business model, network configuration, and operational capabilities.

V. THE COMMISSION SHOULD DEFER ADOPTION OF NEW CYBER ATTACK REPORTING REGULATIONS PENDING THE COMPLETION OF THE CIRCIA IMPLEMENTATION PROCEEDING AT CISA

The Commission should defer revisions to the cyber attack reporting regulations applicable to electric, natural gas, and water utilities pending the completion of proceedings at CISA implementing CIRCIA.[27/] Congress enacted CIRCIA to ensure that, in the aftermath of major cyber incidents affecting critical infrastructure, key cybersecurity policymakers have timely access to accurate information about such incidents in order to assess their potential impact on the public and the nation's economic and national security. The statute established a balanced set of reporting requirements to meet this important objective while avoiding the

[27/] *See* Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 49, 1038-59, 6 U.S.C. § 681 *et. seq.*

potential pitfalls of a regime that encourages over-reporting of incidents.[28/] CIRCIA meets this objective by establishing reporting thresholds focused on entities and incidents that raise significant risks. This approach prevents flooding the government with reports of insignificant incidents, quickly contained incursions, or malicious activity that poses little threat to the operation of critical functions.

As the ANOPR notes, CIRCIA "reflects a comprehensive state-of-the-art approach to critical infrastructure cybersecurity" that could "serve as a model for the PUC's cyber incident reporting obligations."[29/] In accordance with that view, the Commission should forego adoption of new cyber reporting rules pending completion of the CIRCIA implementation proceeding, which is already underway.[30/] That proceeding will yield critical additional insight into key matters, such as identifying the types of entities that constitute "covered entities" subject to reporting obligations and what constitutes a "substantial cyber incident" that triggers such obligations.[31/] These matters are critical to striking the appropriate balance between ensuring that the government has timely and accurate information about substantial cyber incidents while avoiding over-reporting of incursions that have little or no disruptive effects on the public.

In addition, deferring action on incident reporting also aligns with the ANOPR's appropriate concern with avoiding duplicative or overlapping regulation.[32/] This concern is particularly acute for telecommunications companies, which are not only subject to CIRCIA, but

[28/] *See* 6 U.S.C. § 681b (Required reporting of certain cyber incidents); 6 U.S.C. § 681c (Voluntary reporting of other cyber incidents).

[29/] *ANOPR* at 20.

[30/] *See Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022,* Request for Information, 87 Fed. Reg. 55833 (rel. Sept. 12, 2022).

[31/] *Id.* at 55835.

[32/] *See ANOPR* at 21.

also to data breach reporting requirements under the FCC's rules – the latter of which are now under review for possible revisions.[33/] One key issue under consideration in the FCC proceeding is whether to adopt an express harm-based notification trigger.[34/] Harm triggers are common in existing state data breach laws, and they are critical to reducing the risk of over-notification. Both the CIRCIA proceeding at CISA and the FCC proceeding could provide important guidance on the most prudent and workable approaches to achieving the objectives of cyber incident reporting requirements while preventing over-reporting.

[33/] *See Data Breach Reporting Requirements*, Notice of Proposed Rulemaking, FCC 22-102 (rel. Jan. 6, 2023).

[34/] *See id.* ¶¶ 15-22.

CONCLUSION

BCAP appreciates the opportunity to comment on the Commission's efforts to modernize its existing cybersecurity regulations. For the reasons explained above, the Commission should build on the voluntary and flexible standards that are fundamental to successful cybersecurity efforts, ensure that any new or revised rules recognize the Commission's jurisdictional limitations, promote industry standards and best practices, and wait to adopt any new or revised cyber attack reporting regulations after CISA concludes its CIRCIA implementation proceeding.

Respectfully submitted,

/s/ *Todd Eachus*
Todd Eachus
President

BROADBAND COMMUNICATIONS ASSOCIATION
OF PENNSYLVANIA
127 State Street
Harrisburg, PA 17101-1025
(717) 214-2000

February 8, 2023