Joseph Monaghan
Assistant Vice President–
Senior Legal Counsel
AT&T Services, Inc.

1425 US HWY 206
Bedminster, NJ 07921

T: 908-432-8751
jm242x@att.com

Electronic Filing

July 16, 2025

Matthew L. Homsher, Secretary
Pennsylvania Public Utility Commission
400 North Street, Commonwealth Keystone Building
Second Floor – Room N201
Harrisburg, PA 17120

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

Dear Secretary Homsher,

Attached for filing on behalf of AT&T Enterprises, LLC, Teleport Communications America, LLC and SBC Long Distance, LLC (collectively, "AT&T") are Comments in response to the Supplemental Advance Notice of Proposed Rulemaking Order ("ANOPR") dated April 24,2025.

Please contact me if you have any questions.

Respectfully submitted,

Joseph Monaghan
AVP, Senior Legal Counsel

Enclosure
Cc: Colin Scott, Assistant Counsel, Law Bureau colinscott@pa.gov
Chris Van de Verg, Assistant Counsel, Law Bureau cvandeverg@pa.gov
Daniel Searfoorce, Manager (BTUS) dsearfoorc@pa.gov
Michael Holko, Director, Cybersecurity Compliance miholko@pa.gov
Karen Thorne, Law Bureau, kathorne@pa.gov

PENNSYLVANIA
PUBLIC UTILITY COMMISSION
Harrisburg, PA 17105-3265

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

COMMENTS ON BEHALF OF AT&T IN RESPONSE TO PROPOSED RULEMAKING

Pursuant to the Notice issued in the above-referenced matter, AT&T Enterprises, LLC, Teleport Communications America, LLC and SBC Long Distance, LLC (collectively, "AT&T") hereby submit the following Comments to the Public Utility Commission ("Commission").

Introduction

AT&T appreciates the Commission's attention to this critical issue and welcomes the opportunity to submit these Comments in response to the Commission's "Supplemental Advance Notice of Proposed Rulemaking" issued on April 24, 2025, and published in the Pennsylvania Bulletin on May 17, 2025.

AT&T submits that the public interest will be best served by the Commission maintaining its practical approach to cybersecurity preparedness by encouraging utilities to utilize the adaptable NIST Cybersecurity Framework (CSF) to assess and improve their ability to prevent, detect, and respond to cybersecurity risks, rather than imposing specific cybersecurity plan elements inconsistent with the flexibility of the CSF. Imposing added compliance and reporting obligations at the state level would needlessly divert time and resources from the utilities' core efforts to actively defend against cyber-attacks.

Likewise, there is no public benefit to imposing new cyber incident reporting requirements on telecommunications providers already subject to Pennsylvania laws and regulations requiring notice of breaches and service outages. Duplicative reporting obligations would increase the costs for both providers and the Commission without adding any public benefit. AT&T offers the following comments in response to the following numbered questions in Appendix A to the Supplemental ANOPR.

Cybersecurity Fitness Standards

1. Should the Commission require jurisdictional utilities to maintain cybersecurity programs and plans that conform to specific standards and frameworks such as NIST Cybersecurity Risk Framework, NIST Special Publication 800-53, and/or NIST Special Publication 800-82?

AT&T Comments:

The Commission should refrain from promulgating new rules that compel Pennsylvania utilities to prepare cybersecurity plans meeting inflexible prescriptive standards, given that a robust, nationally recognized framework already exists: the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"). Imposing divergent state requirements would undermine security objectives, strain limited resources, and jeopardize the very resilience the Commission seeks to promote.

The NIST CSF provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a catalog of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. Notably, the NIST CSF is purpose-built for critical infrastructure operators, including electric, gas, water, and telecommunications utilities. It is voluntary, risk-based, technology-neutral, and expressly

designed to avoid a one-size-fits-all mandate. Its flexibility enables each utility—regardless of size, complexity, or maturity—to tailor controls to unique operational technology ("OT") and information technology ("IT") environments. By anchoring industry practice in a single federal standard, NIST has cultivated a common cybersecurity language that facilitates information sharing, benchmarking, and continuous improvement across sectors and state boundaries.

In sharp contrast, state-specific prescriptive mandates would fragment that national baseline and create a patchwork of potentially conflicting obligations. Utilities frequently operate across multiple jurisdictions or exchange power, data, and services with entities that do. If Pennsylvania mandates utilities to build duplicative or potentially inconsistent compliance programs, it will divert engineering and security efforts away from threat mitigation and toward paperwork and gap-analysis.

Cyber threats, technologies, and best practices continuously evolve. The NIST CSF's outcomes-based structure solves this by allowing utilities to swap controls as superior approaches emerge, without waiting for a rulemaking. Imposing state-level standards could chill the spirit of voluntary, collaborative cybersecurity improvement that federal policy purposely fosters. The National Security Memorandum on Improving Cybersecurity for Critical Infrastructure and CISA guidance explicitly characterize participation in federal frameworks as non-regulatory, seeking candid engagement and rapid sharing of vulnerabilities without fear of regulatory sanctions. If Pennsylvania converts that guidance into a regulatory floor -- especially if penalties attach -- utilities may become more guarded, limiting the transparency that underpins sector-wide resilience.

Pennsylvania utilities already answer to myriad oversight bodies at the federal level. Adding a state-specific compliance scheme atop those regimes, potentially inconsistent with the

federal policy, would divert limited capital and workforce from tangible security improvements toward redundant audits and reporting. The Commission should embrace CSF and encourage each utility operating in the Commonwealth to take advantage of the CSF resources to develop a plan commensurate with its cybersecurity needs.

Indeed, imposing a set of standards at the state level would conflict with the Commission's long-standing policy of avoiding overlap with federal regulation, and would siphon technical and financial resources from ongoing protection efforts. Each utility should remain free to adopt the federal or industry framework that best fits its operations, and continue to certify to the Commission that it maintains a plan tailored to its needs – and not one with elements mandated by the Commission.

It is noteworthy that the FCC has declined to adopt its own prescriptive cybersecurity requirements in various proceedings in favor of reliance on the NIST CSF. For instance, In the Matter of Establishing a 5G High-Cost Fund for Rural America[1], the FCC simply required that 5G Fund support recipients' cybersecurity risk management plans reflect at least the latest version of National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity and follow the established cybersecurity best practices described in that Framework. Similarly, NTIA, when it developed requirements for applicants in the BEAD program[2], rejected calls for prescriptive cybersecurity requirements and instead relied on the NIST CSF. The Commission's best course of action is to rely on the CSF -- as the FCC and NTIA have done -- to maintain the alignment of state policy with existing federal policy.

---

[1] Federal Communications Commission, GN Docket No. 20-32, FCC 24-89 Second Report and Order, Order on Reconsideration, and Second Further Notice of Proposed Rulemaking at Section IX, paragraph 122 (August 29, 2024).

[2] NTIA Notice of Funding Opportunity, Broadband Equity, Access and Deployment Program at page 70. BEAD NOFO.pdf

It bears noting that the communications sector has a long history of working cooperatively and productively with the federal government to prevent and respond to cybersecurity breaches. Cybersecurity is a significant priority for AT&T; and AT&T defends its network with a multi-layered approach, including monitoring, active prevention, and rapid response to security threats. We leverage tools, where available, that include near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trend analysis and predictive security alerting.

AT&T's network and information security program is designed to protect the confidentiality, integrity and availability of its information and that of its customers. It encompasses the Chief Security Office (CSO) and its policies, platforms, procedures and processes for assessing, identifying and managing risks from cyber threats. This includes third-party risk from vendors and suppliers. The program is designed to identify, respond to and resolve security incidents and threats in a timely manner to minimize the loss or compromise of information assets.

AT&T assesses, identifies and manages risks from cybersecurity threats through various mechanisms and practices. These include vulnerability testing, attack simulation and tabletop exercises to examine our preparedness and incident response process, penetration tests, threat modeling, a Bug Bounty program, large scale data correlation and alerting, and internal and external audits. We conduct vulnerability testing and assess identified vulnerabilities for severity, the potential impact to AT&T and our customers, and likelihood of occurrence. Our security teams work with application and system owners to remediate those vulnerabilities. We regularly evaluate security controls to maintain their functionality in accordance with our security policy. We also obtain cybersecurity threat intelligence from recognized forums, third parties and other

sources as part of our risk assessment process. In addition, as a critical infrastructure entity, we collaborate with numerous agencies in the U.S. government to help protect U.S. communications networks and critical infrastructure. This in turn informs our cybersecurity threat intelligence.

In 2024, AT&T CSO became a Board Member of the National Cybersecurity Alliance (NCA), a nonprofit focused on creating a more secure and interconnected world through various public awareness and educational efforts. AT&T recognizes the importance of harnessing the collective power of our industry to advance network and data security and participates in many security organizations, including:

- Forum of Incident Response and Security Teams
- Internet Engineering Task Force
- Council to Secure the Digital Economy
- National Cyber-Forensics and Training Alliance
- The President's National Security Telecommunications Advisory Committee
- CISA Joint Cyber Defense Collaborative
- NSA Cybersecurity Collaboration Center
- Critical Infrastructure Partnership Advisory Council to protect U.S. communications networks and other infrastructure.

The AT&T Chief Security Office's technical personnel work in partnership with other AT&T business units to evaluate threats, determine protective measures, create response capabilities, and promote compliance with best security practices. AT&T and its employees interact with and participate in several US and international security organizations.

These organizations include:

- Computer Emergency Response Team/Coordination Center (CERT/CC)
- U.S. Department of Homeland Security's National Security Telecommunications Advisory Committee (NSTAC)
- U.S. Department of Homeland Security's Joint Cyber Defense Collaborative (JCDC)
- U.K. National Cyber Security Centre National Security Information Exchange (NSIE)
- Australian Cyber Security Centre (ACSC) National Information Exchange (NIE)
- Various Information Sharing and Analysis Centers (ISACs), including Information Technology-ISAC and Communications-ISAC
- US InfraGard
- Security activities within the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE)
- Cyber Information Sharing and Collaboration Program (CISCP)

At the crux of these efforts to secure its network is AT&T's active participation with other telecommunications providers in the ongoing federal government cybersecurity initiatives, including participation in CISA's painstaking efforts to craft federal rules implementing CIRCIA. As stated above, those efforts have resulted in a robust, nationally recognized framework to assess and address cybersecurity threats that should not be undermined by divergent state requirements.

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?

AT&T Comments:

At its core, the NIST CSF is designed to be flexible so companies of different sizes can apply it in a way that best fits how they operate and the risks they face. If the Commission refrains from imposing mandatory standards, and instead leverages the existing federal resources, there will be no need for additional scaling. Smaller utilities should have proportional obligations reflecting their resources and risk exposure.

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

AT&T Comments:

Depending on the requirements of the proposed rules, waivers might be necessary and should be granted when a utility demonstrates that an alternative framework or control set provides a level of protection commensurate with its risk environment. Given the evolving nature of cybersecurity, the Commission should articulate flexible waiver criteria.

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?

AT&T Comments:

As stated above, the Commission should not dictate any standards. To the extent it does so, utilities that already comply with equal or stricter standards should be deemed to satisfy any new Commission requirement upon annual self-certification to that effect. There should be no doubt that requiring a utility to rework an existing cybersecurity program that follows the CSF or other federal guidance for the sole purpose of satisfying a parallel state rule would be counterproductive.

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?

AT&T Comments:

Smaller utilities should be allowed to opt out of inapplicable standards if they can certify that the risk is adequately mitigated through compensating measures.

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

AT&T Comments:

To the extent the Commission adopts rules tied to an existing federal standard, it should adopt the staff-proposed "automatic update" mechanism only insofar as an updated framework does not impose material new obligations. Where a revision adds substantive requirements, the Commission should first publish a notice and solicit comments before the update becomes enforceable.

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

AT&T Comments:

Annual self-certification remains the most efficient mechanism. Any additional "third-party expert certification" or on-site inspection by Commission staff would be impractical given the scarcity of qualified assessors and the security risks inherent in disclosing proprietary architecture details.

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

AT&T Comments:

The current enforcement tools (e.g., investigations, audit findings, civil penalties) are robust and do not require modification. New prescriptive penalty frameworks are unnecessary

and would risk unnecessarily penalizing utilities for technical non-conformances that pose no actual risk.

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).

AT&T Comments:

"Yes. Annual cybersecurity certifications may contain sensitive information that could aid malicious actors if disclosed. Such information should be protected as Confidential Security Information under applicable Pennsylvania law to safeguard public safety and utility security. "Notably, the best way to combat the risk of unintended disclosure or security practices would be to require minimal information in the Certification.

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?

AT&T Comments:

The Commission should implement secure electronic submission using encrypted portals or secure email gateways. Access must be limited to authorized personnel with a legitimate need to know, and retention periods should be minimized.

Cyber Incident Reporting

5. Are the purposes and design for cyber incident report collection stated by CISA, NOPR at Section III.C. ("Purpose of Regulation"), substantially the same as the Commission's statutory role in ensuring that jurisdictional utilities provide reasonably adequate, reliable, continuous and safe service to the public?

AT&T Comments:

No. CISA's objectives under CIRCIA -- real-time trend analysis, Tactics, Techniques and Procedures identification, and national incident response -- are very different from the Commission's statutory mandate to ensure safe and adequate service. The Commission should not take on the role of analyzing cyber threats or judging the adequacy of a utility's response measure. Doing so would place the Commission in an unnecessary and misplaced role as a gatekeeper to sensitive data that has no relevance to its objectives. Put simply, CISA is focused on national defense and receives and analyzes the information necessary to fulfill its role. The Commission would be overwhelmed by the responsibility of reviewing and securing the data – much of it having no bearing on utility service in Pennsylvania.

6. Identify any role you believe the Commission has to play in each of the following areas:

a. Trend and threat analysis (i.e., the performance of cybersecurity threat and incident trend analysis and tracking, to include the analysis and identification of adversary tactics, techniques, and procedures (TTPs)).

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

c. The provision of early warnings (i.e., the rapid sharing of information on cyber threats, vulnerabilities, and countermeasures through the issuance of cybersecurity alerts or other means).

d. Incident response and mitigation (i.e., rapid identification of significant cybersecurity incidents and offering of assistance—e.g., personnel, services—in incident response, mitigation, or recovery).

e. Supporting Federal efforts to disrupt threat actors; and advancing cyber resiliency (i.e., developing and sharing strategies for improving overall cybersecurity resilience; facilitating use of cyber incident data to further cybersecurity research; engagement with software/equipment manufacturers on vulnerabilities and how to close them).

f. Sharing cybersecurity threat and incident information with utility, state, and federal stakeholders for the purpose of making them aware of cybersecurity threat information

that could impact their critical infrastructure or cause the potential risk to the consumer's health, safety, and/or welfare?

AT&T Comments:

The Commission serves an important role in cybersecurity by encouraging utilities under its jurisdiction to take full advantage of the NIST CSF resources and participate in Information Sharing and Analysis Centers (ISACs). The Commission has the option to subscribe to and redistribute relevant ISAC alerts to those companies that elect to receive them from the Commission, but need not duplicate that function for companies like AT&T who already receive those alerts. This approach allows utilities to receive timely and relevant alerts tailored to their specific needs without imposing prescriptive requirements on which alerts to prioritize or subscribe. The Commission should share threat information with CISA, the FBI, sector ISACs or others as appropriate and coordinate responses with PEMA when requested. However, hands-on threat assessments and responses should remain with the utilities and federal agencies charged with that responsibility.

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

AT&T Comments:

Telecommunications providers should continue to be exempt from reporting cyber incidents to the Commission.

Regulated telecommunications providers are already required to report certain service outages under 52 Pa. Code Section 67.1, which allows the filing of "a comparable outage report required by the Federal Communications Commission" in lieu of certain information required by the rule. Indeed, telecommunications providers are subject to extensive federal oversight and reporting requirements regarding outages and cybersecurity incidents, including obligations to the FCC, CISA, SEC, and law enforcement. Imposing additional state-specific reporting

requirements would be duplicative, create unnecessary administrative burdens, and potentially divert resources from incident mitigation.

Moreover, 66 Pa. C.S. § 3015(e) specifically limits the reports the Commission is authorized to require from a local exchange telecommunications company; and a cyber-attack report is not one of the statutorily permitted reports. 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). Chapter 30 expressly 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," 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."

Given that telecommunications providers already file detailed network outage reports with the FCC's NORS and DIRS systems and are subject to robust federal oversight, layering a separate PUC cyber-incident regime on top of existing federal reporting would be redundant, unnecessary, and in clear contravention of the legislative mandate to reduce regulatory obligations on telecommunications providers.

Likewise, telecommunications providers are subject to 73 Pa. Stat. § 2301, et seq, known as the "Breach of Personal Information Notification Act" (BPINA") -- a robust data breach notification law that was passed in 2005 and recently amended in 2024. Under BPINA, entities that store and maintain "personal information" must provide specified notification following the discovery of certain data breaches to any resident of the Commonwealth and the Pennsylvania Attorney General. Thus, there is no need for the Commission to create an additional notice requirement for a cyber-attack resulting in the possible disclosure of telecommunications customer information.

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?

AT&T Comments:

As stated in AT&T's response to Question 7, there are already rules in place governing the reporting of network outages to the Commission. That should be the primary concern of the Commission, along with breach affecting customer information which is also already addressed by the BPINA. The thresholds for reporting under CIRCIA are focused on incidents that are "substantial" -- those implicating national security interests, foreign relations, the national economy, public confidence, civil liberties, public health, or the safety of the American people. Those matters go beyond the jurisdiction of the Commission; and there is no reason for the Commission to obtain copies of those incident reports.

Eliminating Regulatory Duplication and Overlap

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

AT&T Comments:

Because CIRCIA shall require utilities to compile and submit extensive information, any overlapping state requirement would create unnecessary duplication and divert focus from timely incident response. It would be unproductive to require utilities to draft a second narrative in a different format after already filing one with CISA, and it is unlikely that a state would want or need the same information. The Commission should avoid imposing any state-level incident reporting requirements that would be duplicative, burdensome, or potentially in conflict with federal rules.

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?

AT&T Comments:

See AT&T's response to Question #1.

General

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

AT&T Comments:

Eliminating the cybersecurity elements of Chapter 101, while retaining physical security, emergency response, and business-continuity provisions, will have no negative operational impact provided that the existing self-certification process is preserved elsewhere in the regulations. In fact, removing cybersecurity from Chapter 101 reduces confusion by separating two distinct regulatory tracks.

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.

AT&T Comments:

As demonstrated above and in the federal policy proceedings on this subject, developing and maintaining a cybersecurity plan is an important, time-consuming and costly effort. The costs to utilities if the Commission were to require specific plans, and the costs to the Commission in reviewing and assessing those plans would be enormous. And this is an area that continues to evolve as new threats, and new ways to combat those threats, emerge. Any cost estimate would be obsolete quickly. As discussed above, the NIST CSF already exists to serve the public interest and any public benefit from crafting state-specific rules would be minimal.

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.

AT&T Conclusion:

The Commission can most effectively advance cybersecurity by endorsing, rather than modifying or supplanting, the NIST CSF. Encouraging utilities to leverage the CSF, participate in federal information-sharing initiatives, and integrate lessons from CISA's voluntary Cross-Sector Cybersecurity Performance Goals will promote uniform, flexible, and up-to-date risk management while avoiding the costs and security pitfalls of a fragmented regulatory landscape.

And, finally, for the reasons stated above, telecommunications providers should not and cannot be required to notify the Commission of cyberattacks beyond the existing outage reporting requirements. The federal reporting requirements ensure that relevant authorities are promptly informed and can coordinate an appropriate response. Imposing an additional, state-level notification requirement would not enhance situational awareness or security outcomes but would instead create administrative burdens and slow incident response efforts.

Respectfully submitted,

Joseph Monaghan
AT&T
AVP – Senior Legal Counsel
One AT&T Way
Bedminster, NJ 07921
(908) 432-8751
email: jm242x@att.com

Dated: July 16, 2025