



Joseph Monaghan  
Assistant Vice President -  
Senior Legal Counsel

AT&T Services, Inc.  
One AT&T Way  
Bedminster, NJ 07921

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

February 7, 2023

*Via Electronic Filing*

Rosemary Chiavetta, Secretary  
Pennsylvania Public Utility Commission  
400 North St., 2nd Floor  
Harrisburg, PA 17120

**Re: Docket No. L-2022-3034353  
AT&T Comments in Response to Rulemaking to Review Cyber Security  
Self-Certification Requirements and the Criteria for Cyber Attack Reporting**

Dear Secretary Chiavetta:

Enclosed for filing are Comments on behalf of AT&T Corp., Teleport Communications America, LLC and SBC Long Distance, LLC (collectively, "AT&T") in response to the Public Utility Commission's "Advance Notice of Proposed Rulemaking" in the above-referenced matter.

Thank you for your attention to this matter. Please contact me if you have any questions regarding this filing.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "J. Monaghan".

Joseph Monaghan

Attachment

cc: Colin Scott, Assistant Counsel, Law Bureau (via email)  
Chris Van de Verg, Assistant Counsel, Law Bureau (via email)  
Daniel Searforce, Manager, Bureau of Technical Utilities Services (via email)  
Michael Holko, Director, Office of Cybersecurity Compliance and Oversight (via email)  
Karen Thorne, Law Bureau (via email)

**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 Corp., 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 important issue and welcomes the opportunity to submit these Comments in response to the Commission’s “Advance Notice of Proposed Rulemaking” (“ANOPR”) in this matter. AT&T submits that the public interest will be best served by the Commission maintaining its pragmatic approach to monitoring utilities’ cybersecurity preparedness through the existing annual Self-Certification process. Enacting burdensome state regulations in an area where there is already robust federal oversight would be redundant and needlessly divert time and resources from the utilities’ essential work in guarding their facilities against cyber attacks. The existing Commission regulations, including the Self-Certification process, provide sufficient Commission oversight without intruding on federal regulation and without hampering efforts of utilities focused on the protection of their infrastructure. It is against this backdrop that AT&T offers the following comments in response to the Commission’s numbered topics in Appendix A to the ANOPR.

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

**AT&T Response:** The existing regulations, coupled with efforts at the federal level which will generate even more information for state commissions, are sufficient to address the preparedness of public utilities to address evolving cybersecurity threats. As discussed in the ANOPR, in developing the current regulations, the Commission “endeavored not to replicate regulations that were already in place and required by the Federal government or other agencies but acknowledged its duty to identify and secure critical utility infrastructure and key assets within the Commonwealth.” That should remain the guiding principle in determining whether any revisions to the Commission’s existing cybersecurity regulations are necessary.

To that end, AT&T recommends that the Commission assess the information sharing resources and tools to be rolled out under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCIA”) and existing public-private partnerships in this arena. CIRCIA, which was signed into law in March 2022, creates a statutory framework requiring owners of covered critical infrastructure to report covered cyber incidents and ransomware payments to the Department of Homeland Security (“DHS”). Among other things, CIRCIA directs the Cybersecurity and Infrastructure Security Agency (“CISA”) to begin a rulemaking within twenty-four months of CIRCIA’s enactment. CISA then has eighteen months to finalize the proposed rules. This rulemaking will determine who must report, what information must be reported, and how those reports may be made, thus creating the landscape of cybersecurity resources at the federal level. Those resources will be available to the Commission and utilities without the need for duplicative state-level reporting and local regulation.

## Updating Terms and Concepts

**Topic No. 2: The PUC seeks comment on whether and how to update the terms and concepts used in the existing regulations to better reflect the current cybersecurity landscape, Federal and industry standards and any revisions which may be adopted in this rulemaking.**

**AT&T Response:** As noted in response to Topic No. 1, the CISA rulemaking will establish a national set of terms and concepts reflecting the current cybersecurity landscape. As noted in the ANOPR, “CIRCI A reflects a comprehensive, state-of-the-art approach to critical infrastructure cybersecurity”. The Commission should await CISA’s work on associated regulations at the federal level, rather than attempting now to update terms and concepts in the Commission’s existing regulations.

## Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities

**Topic No. 3: The PUC seeks comment on the relative merits and weaknesses of each of the approaches within the heading “Exploring Approaches to Ensuring Cybersecurity Fitness in Public Utilities” and which of these approaches, some combination of these approaches, or some other approach, provides the PUC, the utility and its ratepayers with the greatest potential assurance that a utility is adequately prepared to address cyber security threats.**

**AT&T Response:** AT&T submits that the public interest is best served by the Commission maintaining the current Self-Certification regime through either of the first two approaches outlined in the ANOPR:

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

We understand that public utilities have successfully implemented the current approach, and expect that utility cybersecurity plans and programs will continue to improve in the wake of CIRCIA and enhanced information sharing at the national level. The Commission will have ample opportunity to benefit from that work at the federal level without burdening utilities with additional reporting requirements at the state level.

Not only is the current regulatory approach sufficient, but each of the other three approaches suggested in the ANOPR are flawed for the following reasons:

*Approach #3: Requiring a public utility to provide a “third-party expert certification.”*

For a company the size of AT&T, and likely for the majority of utilities, it is unworkable to hire a third-party expert to conduct an annual certification. A single audit of companies with the amount of information technology infrastructure that AT&T operates can take many months to complete. It is not practical to conduct a multi-month audit of every utility every year. Among other things, there is not enough third-party expertise in cybersecurity to find experts to do an annual audit of every utility. Moreover, given that significant modifications to information technology infrastructure are often accomplished as long-term projects, there is not enough change to systems, plans and programs from year to year to justify a costly annual expert review.

Third-party assessments are performed regularly across AT&T as part of our cybersecurity program, which incorporates industry security standards. Our internal requirements set a broad minimum level of security, but additional and/or stricter controls (which may include third party review) are used where appropriate, where required by law, and/or as part of third-party agreements.

*Approach #4: Incorporating an onsite review of cybersecurity measures, plans, and programs.* Onsite reviews by commission staff would create a security risk in and of itself and would provide little insight. Moreover, most cybersecurity tools and systems are managed virtually so there is really no “onsite” environment where Commission staff could observe cybersecurity measures.

*Approach #5: Requiring a public utility to file a confidential copy of its cybersecurity plans and programs.* Given the highly confidential nature of the subject matter, AT&T does not widely share the contents of its Security Program and Requirements (ASPR) or its other security policies. Moreover, if the Commission were to take possession of the confidential cybersecurity plans of all utilities under its jurisdiction, the Commission itself would immediately become a prime target for bad actors as the Commission would hold the roadmap to attack utilities in the Commonwealth. The increased risk to the Commission infrastructure would far outweigh the value of holding copies of those plans and programs. Again, that is one of the reasons that the existing Self-Certification regime is the best way for the Commission to regulate utilities in the cybersecurity landscape.

**Topic No. 4: The PUC welcomes comments describing the approaches taken by other state public utility commissions to address public utilities’ cybersecurity fitness and evaluating their respective costs and benefits.**

**AT&T Response:** AT&T notes that cybersecurity and incident reporting is a topic of priority for many states. While other states have considered enhanced requirements for public utilities, they are also keenly aware of the ongoing federal efforts, particularly the CIRCIA rulemaking process currently underway. We urge the PUC to await the outcome of that comprehensive rulemaking before considering additional requirements to public utilities.

**Topic No. 5: Would changes to the cybersecurity aspect of 52 Pa. Code § 101.3 impact the physical security, emergency response and/or business continuity aspects of the rule and/or Chapter 101 generally? The PUC seeks comment on the nature and extent of such foreseeable impacts and ways to address those impacts.**

**AT&T Response:** Again, AT&T submits that the regulation at 52 Pa. Code § 101.3 should not be changed unless and until any changes are required to conform those rules to remain consistent with rules being developed at the federal level. Notably, the existing language of section 101.6(d) of the regulations is an important aspect that should remain in place to eliminate duplication of efforts. Specifically, that section provides that a public utility “that has developed and maintained a cyber security, physical security, emergency response or business continuity plan under the directive of another state or Federal entity that meets the requirements of § 101.3 (relating to plan requirements) may utilize that plan for compliance with this subpart, upon the condition that a [PUC] representative be permitted to review the cyber security, physical security, emergency response or business continuity plan.”

#### **Improving the Self-Certification Form (SCF) Process**

**Topic No. 8: The PUC seeks comment on ways to streamline and otherwise improve the filing, handling, and storage of SCFs.**

**AT&T Response:** AT&T has not encountered any issues in the filing of its annual SCF filings. Certainly, the Commission should ensure that it is storing SCFs and any related materials in a secure manner to guard against access by bad actors.

**Topic No. 9: The PUC seeks comment on whether and how to streamline the self-certification form, plan and reporting requirements to better calibrate the benefits of the existing regulations against the burdens they place on regulated entities, especially smaller utilities, and on PUC staff.**

**AT&T Response:** See response to Topic No. 8.

## Updating Cyber Attack Reporting Regulations

**Topic No. 10: The PUC seeks comment on potential ways to revise the reporting criteria in its existing regulations, including the potential addition of new requirements for reporting incidents involving IT.**

**AT&T Response:** The existing regulations properly do not apply to AT&T or other telecommunications utilities; and the Commission should **not** expand those regulations to include telecommunications utilities. The communications sector has long-standing partnerships with the federal government to address cybersecurity dating back to the 1960s following the Cuban Missile Crisis when President Kennedy prioritized protecting the nation's communication infrastructure. This lengthy history distinguishes the communications sector from others. These partnerships are largely driven by the National Security Telecommunications Advisory Committee ("NSTAC"), the Comms-Sector Coordinating Council ("CSCC"), and the National Coordinating Center for Telecommunications ("NCC") Communications Information Sharing and Analysis Center ("Comms-ISAC"). Additional collaborative efforts include the Computer Emergency Response Team/Coordination Center ("CERT/CC"); the Forum of Incident Response and Security Teams ("FIRST"); the Enduring Security Framework ("ESF") (a public private partnership between industry and various Federal agencies intended to improve cybersecurity); the U.K. Centre for the Protection of National Infrastructure ("CPNI"); National Security Information Exchange ("NSIE"); various Information Sharing and Analysis Centers ("ISACs"), (including the Information Technology, Auto, and Retail ISACs); and the Joint Cyber Defense Collaborative ("JCDC") (a collaborative effort between the federal government and private sector to gather and share actionable cyber risk information to better support cybersecurity planning, defenses, and response).



These efforts are representative of the ongoing collaboration between industry and government that has been the traditional means for enhancing cybersecurity. Bolstered by federal statutory authority and liability protections, cyber threat information sharing has traditionally been done on a voluntary basis. CIRCIA's narrowly drawn incident reporting regime was designed to provide CISA with information about significant incidents such that it may be able to help mitigate impacts of novel threats to other entities. It is a carefully struck balance between the traditional voluntary information sharing regime and congressional desire for more consistent reporting to DHS about certain incidents.

CISA intends to receive actionable cybersecurity incident information from critical infrastructure providers, triage the information, and push information and recommendations back to the industry with the intent of improving the cybersecurity ecosystem for all operators of critical infrastructure (i.e., a public-private partnership approach). And states already have the ability today to engage in an information exchange program with DHS through the Multi-state Information Sharing and Analysis Center ("MS-ISAC").

AT&T also notes that while CIRCIA is the first critical infrastructure-wide reporting regime created by statute, the FCC already requires communication providers (wireline, cable, satellite, wireless, interconnected VoIP and Signaling System providers) to report network outages (including a root cause analysis) that satisfy certain thresholds in the FCC's Network Outage Reporting System ("NORS"). The Public Safety and Homeland Security Bureau's Cybersecurity and Communications Reliability Division routinely analyzes NORS data to assess the magnitude of major outages, identify trends, and promote network reliability best practices that can prevent or mitigate future disruptions. And all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have security breach notification laws that require

businesses to notify consumers and the appropriate government entity if personal information is breached.

Thus, there is already robust reporting of the scope and magnitude of communications service interruptions which provides insight into the reliability and resiliency of communications networks and systemic vulnerabilities and threats to communications infrastructure. The Commission can expand its cybersecurity awareness and resources by participating in information sharing with DHS via MS-ISAC or other federal-state mechanisms. Being keyed into DHS's information-sharing when DHS pushes out threat warnings and protective measures will help the Commission be a partner in protecting utilities within its jurisdiction.

The Commission also should participate in CISA's NPRM process to represent interests of the Commonwealth. As CISA becomes a centralized source of information regarding significant cyber incidents involving critical U.S. infrastructure, the Commission should ensure CISA prioritizes the sharing of useful information in real-time and offers tools and assistance, otherwise inaccessible, about cybersecurity incidents affecting the Commonwealth, thus obviating the need for redundant regulation and reporting at the state level.

### **Merging the Self-Certification and Cyber Attack Reporting Regulations**

**Topic No. 12: The PUC seeks comment on the pros and cons of merging the self-certification and cyber incident reporting regulations into a single chapter of the Code, and otherwise eliminating unintended or unjustified inconsistencies in the existing regulations.**

**AT&T Response:** As discussed above, the current cyber attack reporting requirements do not appear in the Code chapter governing telecommunications utilities. And it should remain that way for the reasons stated above. As such, any merging of the self-certification and incident reporting regulations may create confusion as to which entities are covered by each requirement

with no apparent benefit to the merging of the sections. There is an important and rational basis to treat utilities differently in the Code and there is no reason to blur that distinction in this case.

### **Cost-Benefit Analysis**

**Topic No. 13: The PUC seeks comment on how best to justify revisions to the existing regulations under the Regulatory Review Act standards. In particular, the PUC seeks comment on how the costs and benefits associated with its existing regulations, and any revisions thereto, can be objectively quantified and evaluated.**

**AT&T Response:** It is premature to comment on any costs or benefits associated with any revisions, but AT&T offers as a general comment that to the extent there are revisions imposing additional regulatory reporting obligations on utilities, it should be possible to quantify the costs associated with those burdens. From AT&T's standpoint, any additional regulatory costs levied upon its regulated businesses, at a time when customers are already moving to non-regulated services, will make it that much harder to compete against non-regulated companies offering competitive services. In addition, imposing costly reporting obligations on utilities diverts resources from the work being devoted to securing infrastructure, which should be the paramount goal of any regulatory activity in the cybersecurity landscape.

### **Eliminating Regulatory Duplication and Overlap**

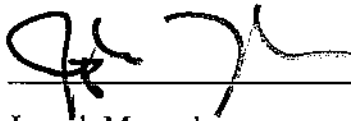
**Topic No. 14: The PUC seeks comment on the potential for conflict, overlap, redundancy, or other bases warranting review in the interplay between the PUC's cybersecurity regulations (and revisions thereto) and Federal initiatives, including but not limited to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).**

**AT&T Response:** See above responses to Topic Nos. 1, 3 and 10.

**Conclusion**

The Commission should refrain from expanding existing reporting obligations imposed on telecommunication providers at this time. Instead, it should focus on participating in the CISA rulemaking to ensure that CISA appropriately deploys resources and assistance to states, timely identifies emerging cyber threats and trends, and quickly shares threat information with other Pennsylvania entities to mitigate broader impact across communication networks in the Commonwealth.

Respectfully submitted,



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

Dated: February 7, 2023