



417 Walnut Street
Harrisburg, PA 17101
717 255-3252 / 800 225-7224
FAX 717 255-3298
www.pachamber.org

The Honorable Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
400 North Street
Harrisburg, PA 17101

Feb. 7, 2023

RE: Advance Notice of Proposed Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Docket L-2022-3034353 (52 Pa.B. 7507)

Dear Secretary Chiavetta,

On behalf of the Pennsylvania Chamber of Business and Industry (PA Chamber), the largest, broad-based business advocacy organization in the commonwealth, representing nearly 10,000 member companies of all sizes and all commercial and industry sectors, thank you for the opportunity to submit comments regarding the Pennsylvania Public Utility Commission's Advance Notice of Proposed Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting, Docket L-2022-3034353, as published for comment in the Dec. 10, 2022 edition of the Pennsylvania Bulletin (52 Pa.B. 7507).

The PA Chamber's interest in this matter is to support policy that ensures the affordable, safe and reliable gas, electric, water and telecommunications utility service to our members. With cybersecurity an on-going and emerging threat to business operations, we sincerely appreciate the Commission's efforts to ensure regulated utilities have appropriate safeguards with respect to cybersecurity. The PA Chamber respectfully submits the following comments for the Commission's consideration as it formulates a final proposed regulation.

The Commission's Existing Approach Should Be Applauded and Reinforced

Generally speaking, the existing regulations rightly recognize there is no "one-sizes-fits-all" approach that is appropriate to require of every regulated utility. The non-prescriptive nature of these regulations, notably the use of a self-certification, is logical and appropriate, especially given the requirements already imposed on utilities by financial institutions and insurers to ensure operational continuity and mitigation of financial losses due to a data breach or disruption. Should the Commission amend the regulations, the new requirements should to the greatest extent possible avoid duplicative regulatory requirements already in place, such as those established by federal law.

The existing regulations also recognize that in many cases an incident involving cybersecurity may also involve a disruption to service that mirrors already reportable incidents in which safety or soundness of the regulated utility infrastructure is implicated.

Ms. Rosemary Chiavetta, Secretary
Comments of the PA Chamber re Cyber Security Rulemaking
Docket No. L-2022-3034353
Feb. 7, 2023

The PA Chamber Supports a Regulatory Approach that Continues to Emphasize Self-Certification and Reporting

The ANPR outlines five potential regulatory approaches for the Commission to adopt and for interested parties to provide comment on. The PA Chamber generally supports the first of these five options, as written: “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.”

For the reasons stated above, a regulatory approach that continues to provide for self-certification and annual reporting satisfies the Commission’s statutory charges and recognizes the on-going efforts by utilities and their vendors to ensure risk from cybersecurity is minimized and that appropriate response measures are in place in the event of an incident.

Since the promulgation of the Commission’s existing regulations governing cybersecurity, there have not been incidents sufficient to justify a significant change in approach. Further, the other four possible regulatory approaches published for comment do not include a cost-benefit justification as required by the state’s Regulatory Review Act. While we understand such an analysis would accompany a full proposed rulemaking once submitted to IRRC, at this point we do not believe additional regulatory requirements as contemplated in the other options would provide a meaningful benefit.

* * *

In closing, thank you for the opportunity to file comments on this important matter. We thank the Commission for its efforts to address risks from cybersecurity, and look forward to continue working with the Commission and our members on this important issue.

Sincerely,



Kevin Sunday
Director, Government Affairs