STATE OF MARYLAND

PUBLIC SERVICE COMMISSION

March 27, 2024

Chair Brian J. Feldman
Education, Energy, and the Environment Committee
2 West, Miller Senate Office Building
Annapolis, MD 21401

RE: HB 1420 – Unfavorable –- Cybersecurity – Office of People's Counsel, Public Service Companies, Public Service Commission, and Maryland Cybersecurity Council

Dear Chair Feldman and Committee Members:

During the 2023 Session, the Maryland General Assembly enacted House Bill 969 (HB0969) entitled, "Public Service Commission – Cybersecurity Staffing and Assessments (i.e., the "Critical Infrastructure Cybersecurity Act of 2023" or "the Act").[1] As introduced, the Act was focused on requiring public service companies to implement certain cybersecurity standards, conduct independent third-party cybersecurity assessments every two years and report cybersecurity incidents to the Maryland Department of Information Technology (DoIT) Office of Security Management, among other things. HB0969 was codified in Public Utilities Article (PUA), § 2-108 and §5-306, Annotated Code of Maryland, which was enacted July 1, 2023. The Commission has a rulemaking session scheduled March 27, 2024, to codify these statute requirements in COMAR.

HB 1420 introduces definitions currently not codified in PUA § 5-306 for critical software and supply chain risk. HB 1420 then requires an assessment of critical software when public service companies engage with a third party to conduct an assessment of their cybersecurity standards adherence every two years as currently required by PUA § 5-306. HB 1420 also requires that public service companies establish minimum standards for supply chain risks. Finally, HB 1420 defines cyber resilience and requires that cyber resilience be added to service quality and reliability standards in PUA § 7-213. HB 1420 also adds a definition for critical infrastructure but does not have any direct requirements in the bill related to this definition.

Without commenting on OPC's needs to participate in cybersecurity matters associated with the Commission's implementation of PUA § 5-306 changes established in CY2023, other aspects of the bill are either redundant with existing PUA § 5-306 requirements, or are not needed.

The current definitions of operational technology and information technology systems, in COMAR 20.06 are already included in the scope of third-party assessments of public service company standards

[1] Delegate Qi sponsored HB 969. Senator Hester introduced the identical cross-file to HB0969 as Senate Bill 800.

adherence every two years. Operational technology and information technology system assessments include software. Therefore HB 1420's requirements for critical software are not needed.

Furthermore, supply chain risk does not need to be given additional emphasis in HB 1420 since PUA § 5-306(c)(3) already requires the establishment of minimum-security standards for supply chain risks.

In addition, the addition of cyber resilience in PUA § 7-213 is misplaced as this section of the Maryland Annotated Code is primarily related to electric utility reliability, not cybersecurity. Codification of cyber resilience in a section of the Maryland Annotated Code related to electric utilities misses the fact that PUA § 5-306 cybersecurity requirements are applicable to all public service companies, including gas and water utilities. Therefore, this statute requirement would not apply to water and gas public service companies that are subject to PUA §5-306.

Finally, the addition of cyber resilience requirements is not needed because the utility periodic assessments required by PUA § 5-306 every two years already need to be performed using either the Cybersecurity and Infrastructure Security Agency's Cross-Sector Cybersecurity Performance Goals (CPG) or a more stringent standard that is based on the National Institute of Standards and Technology (NIST) security frameworks. Both the CPG and NIST frameworks for assessments include an evaluation of the ability of a public service company to identify, protect, detect, respond, and recover from cyber-attacks, which is synonymous with the intent of the HB 1420 definition for cyber resilience[2]. Therefore, the cyber resilience requirement in HB 1420 is not needed.

I appreciate the opportunity to provide unfavorable testimony on HB 1420. Please contact the Commission's Director of Legislative Affairs, Christina M. Ochoa, at christina.ochoa1@maryland.gov if you have any questions.

Sincerely,

Frederick H. Hoover, Chair
Maryland Public Service Commission

[2] In HB 1420, "Cyber resilience" means the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.