STATE OF MARYLAND

OFFICE OF THE CHAIRMAN

JASON M. STANEK

PUBLIC SERVICE COMMISSION

March 7, 2023

Chair Brian Feldman
Education, Energy and Environment Committee
2 West, Miller Senate Office Building
Annapolis, Maryland 21401

RE: SB 800 – INFORMATION – Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)

Dear Chair Feldman and Committee Members:

SB 800 requires the Maryland Public Service Commission to include one or more cybersecurity experts on its Staff to advise the Commission and perform certain duties, collaborate with the Office of Security Management ("OSM") to establish cybersecurity standards and best practices for regulated entities, share cybersecurity-related information and best practices with municipal electric utilities, require certain public service companies to adopt and implement cybersecurity standards and conduct assessments, and require the Commission to conduct and submit an evaluation of the public service companies' assessments to OSM and the Maryland Department of Emergency Management ("MDEM").

In 2019, the Commission established a three-year audit cycle framework for periodic cybersecurity reporting based recommendations from a two-year stakeholder process. All applicable Maryland utilities have completed their first cycle of briefings.[1] On July 25, 2022, the Commission adopted cybersecurity regulations that incorporate critical lessons learned from the cybersecurity reports. Maryland thus became only the third state in the nation to promulgate cybersecurity regulations for its public service companies, consistent with President Biden's request to State Governors on March 18, 2022, to promulgate standards to secure critical infrastructure, among other things.

The Commission will need to hire three cybersecurity experts to perform the mandates of SB 800. The specific duties and responsibilities of these experts listed in Section 2-108(d)(3)— include, among other things, advising the Chairman and the Commissioners on cybersecurity, studying and monitoring cybersecurity best practices, and assisting in drafting cybersecurity-

[1] Commission issued Order No. 89015 on February 4, 2019, establishing various cybersecurity definitions and establishing a three-year audit cycle framework for periodic cybersecurity reporting to the Commission by Maryland electric, gas, or water companies that have 30,000 or more customers in Maryland. In addition, the Commission established a cybersecurity breach reporting protocol for all Maryland electric, gas, and water companies under their jurisdiction.

related regulations—and are inherent to the unique technical and advisory role of Commission Staff. These functions are best integrated in the Commission's hiring documents, pursuant to State personnel procedures, rather than in statute. **The Commission therefore recommends simplifying the language under subsection (d)(3), by striking (I)-(VII), to be consistent with comparable subsections (d)(5) and (d)(6) of Section 2-108. Finally, the Commission would also require an appropriation for the PINS and appropriate salaries** (or condition the hiring of the personnel on the availability of these resources).

Specifically, where SB 800 calls for the technical cybersecurity expert to convene workshops with public service companies that fail to meet the minimum cybersecurity standards in (d)(3)(VI), this requirement is unnecessary. The Commission is authorized under the *Public Utilities Article* to impose an appropriate civil penalty for a violation of law, Commission order, or regulation, as well as require a public service company to file a corrective action plan as opposed to conducting a workshop.[2]

Some of the information sharing requirements in SB 800 raise confidentiality concerns. Under the *PUA*, the Commission has broad oversight authority over public service companies.[3] Cybersecurity matters are extremely confidential, including how breaches are reported, and the Commission has emphasized the proper safeguarding of this information. SB 800 requires the Commission to evaluate the utilities' security assessments of its own operational and informational technologies and submit this evaluation to the OSM and MDEM. Notwithstanding the scope of authority given to DoIT and MDEM, expanding the number of agency representatives with knowledge of a utility's cybersecurity and data privacy threat protections weakens its ability to safeguard this critical information. **Therefore, the Commission recommends striking 2-108(d)(8)(IV).**

SB 800 requires public service companies to adopt NIST security frameworks, which may be unreasonable and burdensome for some utilities, especially smaller ones. While the NIST framework is appropriate for larger utilities, alternative frameworks have been developed for smaller utilities.[4] The COMAR regulations provide utilities the ability to utilize the cybersecurity framework applicable to its situation as opposed to prescribing a "one size fits all" approach.[5] Where Maryland's larger investor-owned utilities manage cybersecurity at the enterprise level across multiple affiliate companies operating in several states, prescriptive and narrowly focused requirements at the state level may be incompatible with broader corporate cybersecurity policy, strategy, and operational requirements for multi-state public utilities. This may require significant utility resources solely for compliance with the Critical Infrastructure Security Act of 2023, without producing any net cybersecurity improvements. **The Commission recommends replacing "based on the National Institute of Standards and Technology Security Frameworks" in (C)(4)(I) with "based on industry-accepted cybersecurity frameworks."**

[2] Public Utilities Article (PUA) Sect. 13-201(b)(1).
[3] PUA Sect. 2-113.
[4] American Water Works Association's ("AWWA") Cybersecurity Guidance and Assessment Tool for small water utilities or the National Rural Electric Cooperative Association ("NRECA") Essence Cybersecurity Tool for smaller electrical cooperative utilities.
[5] COMAR 20.06.01.01.

Additionally, the third-party utility audits required in (C)(4) would involve substantial costs that will be passed on to ratepayers. Finally, notwithstanding the previous concerns, the Commission notes that *annual* cybersecurity assessments of public service companies are an expensive undertaking. **A cybersecurity assessment every three years is more appropriate and aligns with the North American Electric Reliability Council ("NERC") Critical Infrastructure Protection ("CIP") audit frequency for electric transmission.**

I appreciate the opportunity to provide information on SB 800. Please contact Lisa Smith, Director of Legislative Affairs, at (410) 336-6288 if you have any questions.

Sincerely,

Jason M. Stanek
Chairman