Cyril W. Draffin, Jr.
Energy Initiative Project Advisor, Massachusetts Institute of Technology

Testimony in Support of

SB800, "Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)**"**
Sponsor: Senator Katie Fry Hester

Senate Education, Energy, and Environment Committee
1 p.m. March 7, 2023

Thank you for the opportunity to provide testimony in support of Senate Bill 800 pertaining to cybersecurity and the Maryland Public Service Commission (cross-filed with HB069).

My name is Cyril Draffin. I am a Project Advisor on cybersecurity, and serve as a member of the Maryland Cybersecurity Council.

The state needs its utilities to be reliable and protected against cybersecurity threats and attacks. We do not want future successful cyber-attacks on our infrastructure by foreign or domestic entities because the Public Service Commission ("PSC") had not been attentive enough to the cybersecurity programs of the electric, gas, water, and other utilities they oversee.

SUPPORT

Senate Bill 800 has several positive provisions, and requires only modest cost and employee resources.

The bill has provision for assuring one or more of the PSC's employees are experts in cybersecurity to advise the Commissioners, consult with the Maryland Office of Security Management, study cybersecurity best practices, assist in drafting cybersecurity regulation, and assist the PSC in monitoring public service company's security standards. This expertise, missing from current Commission staffing, is needed to provide adequate understanding of the challenges and appropriate actions to defend Maryland utilities from cyber-attack or inadequate cyber planning.

The bill has provision to establish and share cybersecurity standards and best practices, and prepare an evaluation of utilities cybersecurity policies, procedures, and expertise. To date no formal or written cybersecurity report about utilities is prepared and made available to key Maryland departments (even on a confidential basis). Only a quick verbal presentation is made to Commissioners with no written documentation provided for further review.

The bill has a provision for zero trust and assessment based on NIST (National Institute of Standards and Technology) framework for cybersecurity protection. This recognizes that ongoing trust in a system should not be assumed, and system must be regularly evaluated because malicious actors (e.g., employees with malicious intent, external people and organizations, foreign governments) can penetrate perimeter firewalls and reach the insides of information technology or operational technology systems. Maryland utilities need to keep up with evolving cybersecurity and physical security threats.

SUPPORT WITH SUGGESTED AMENDMENTS

The bill has a provision that every two years a third-party with cybersecurity expertise should assess the operational technology and information technology of utilities serving Maryland customers, and that it should be shared with the Maryland Department of Information Technology and the Maryland Department of Emergency Preparedness. This assures an independent evaluation is conducted, and Maryland does not only rely on the good intentions and verbal statements of their utilities.

However, we do not want Critical Energy Infrastructure Information (CEII) from cybersecurity assessments to be made public.

A suggested amendment is for SB 800 to have language restricting release of CEII as part of Freedom of Information Act (FOIA) and other public disclosure requests.

This CEII protection has already been adopted in other states for many years. For instance in 2019 the National Governors Association report (their most recent CEII report) "State Protection of Critical Energy Infrastructure Information (CEII)" (https://www.nga.org/publications/state-protection-of-critical-energy-infrastructure-information-ceii/) indicated that 31 states had "open government law" exemptions that protect CEII. Maryland does provide that protection.

Additional details:

- From National Governors Association report: "Twenty-eight states have adopted statutory exemptions from open government laws for critical infrastructure information (CII, defined as systems and assets, whether physical or virtual, so vital that their incapacity or destruction would debilitate social or economic security; CEII is a subset of CII). Three other states, Hawaii, Minnesota, and Washington, do not explicitly exempt CEII, but language from court cases, opinion letters or general statutory language is interpreted to contain this exemption. Only a few states list a specific state

agency and/or authority that is exempted from open disclosure requirements (e.g., Iowa)."

- Federal Energy Regulatory Commission's policy regarding Critical Energy/Electric Infrastructure Information (CEII) is available on their web site: (https://www.ferc.gov/ceii).
- U.S. Cybersecurity & Infrastructure Agency (CISA) and other Federal organizations release advisories, and patches that the PSC may then forward to utility service providers; and PSC needs to know how these interventions are working to enhance cybersecurity. Sharing assessment information on utilities operating in Maryland with the PSC results in a more informed PSC.
- The Federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires covered entities to report cyber incidents to the Federal government.
- The PSC assessments provided to the State should include anonymous information when it reports on its evaluations.
- Limitations needed to avoid publicly disclosing cyber infrastructure information under the Maryland Public Information Act.

If language protecting CEII information is not added in Maryland, then written reports on cybersecurity of utilities should be marked "Confidential" and not be shared with other Maryland departments or the public.

A second amendment is to delay "Beginning on or before October 1, 2023, and every 2 years thereafter, evaluate the assessments…" (SB800, page 5, line 7) by six months until April 1, 2024 because bill will not become effective until October 1, 2023 (page 8, line 10).

SUMMARY

SB 800 is a straightforward way to address and improve the cybersecurity readiness of public utilities operating in Maryland.

Because of the need for improved cybersecurity reviews by the Maryland Public Service Commission, I encourage a favorable report on Senate Bill 800-- with the two amendments including adding a provision for Maryland to protect CEII information. I support the committee's continued attention to cybersecurity and physical security of utility operations in Maryland.