KATIE FRY HESTER
Legislative District 9
Howard and Montgomery Counties

Education, Energy, and
Environment Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 · 301-858-3671
800-492-7122 *Ext.* 3671
KatieFry.Hester@senate.state.md.us

Testimony in Support of SB800 - The Critical Infrastructure Cybersecurity Act of 2023

March 7th, 2023

Chair Feldman, Vice Chair Kagan, and members of the Education, Energy, and Environment Committee, thank you for your consideration of SB800, the Critical Infrastructure Cybersecurity Act of 2023.

Last year, the General Assembly took a major step towards improving our state's cybersecurity posture by modernizing systems, extending state resources to units of local government, and by establishing minimum security standards and protocols for our state agencies. However, cybersecurity risk affects every single public and private sector enterprise. As the Colonial Pipeline and Oldsmar, Fl, events have shown us, our critical infrastructure - especially our water, gas, and electrical utilities - are major targets for malicious actors.

In fact, the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security has warned states that these evolving, persistent threats pose "severe physical and economic harm." I have uploaded a 2-pager as part of my testimony that sketches out these threats which include, but are not limited to, cybersecurity risk, supply chain risk, and physical risk.

Broadly, this bill seeks to mitigate cybersecurity risk by drawing upon years of research by the Maryland Cybersecurity Council and its Critical Infrastructure Subcommittee. Specifically, in 2021, the Council commissioned a Fellow from the National Security Administration, Laura Corcoran, who is here today as part of my panel, to study the gaps in our regulation of utilities' cybersecurity standards. While drafting this report, she consulted the Public Service Commission, other state agencies, the best practices of other states, and other research. Then, when the PSC issued new cybersecurity regulations in 2022, I worked with the PSC and the Council's Critical Infrastructure Subcommittee to compare those regulations with the Fellow's recommendations.

This process took several months, and we ultimately identified the highest priority recommendations that were missing from PSC regulation into the bill you see before you today. During these conversations, we uncovered some worrying gaps in PSC's regulatory authority and staff capacity. First and foremost, the Commission does not receive the documentation necessary to have an informed conversation with utilities about their cybersecurity posture. Right now, the Commission receives cybersecurity briefings by utilities infrequently – once every three years. These briefings are closed

and oral only; the Commission keeps no written reports or minutes to examine, and there are no follow-up visits or audits to address how security challenges are being addressed. This process is out of step with other agencies' record-keeping, compliance, or transparency practices.

So what does SB800 do to address these gaps? The bill's provisions fall into three main buckets:

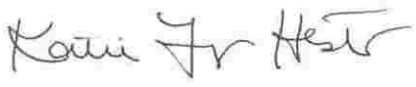
1.) **Requirements on the PSC**. This bill adds "cybersecurity" as one of the seven factors that the Commission must consider when exercising its regulatory power, and requires the Commission to collaborate with the Office of Security Management to establish minimum cybersecurity standards for utilities based on the particular needs of the sector, as well as the size of individual companies. It also requires the PSC to hire at least one subject matter expert in the cyber field to assist in drafting cyber regulations, monitor compliance with minimum standards, and to prepare reports for the Commission's review. This individual would also support utilities in their efforts to improve the maturity of their cybersecurity enterprise.

2.) **Requirements on utility providers.** In addition to requirements on the PSC, this bill would require utility companies to establish minimum security standards for each peripheral device on their networks, commensurate with their risk. These standards would include moving toward a zero trust architecture, and must be used to manage supply chain risk. Many of our larger utilities are already doing this work, but in cybersecurity, you really are limited by your weakest link.

3.) **Reporting requirements.** Finally, this bill would establish two reporting requirements - one for utility companies, and one for the PSC. Specifically, this bill would require each utility company in the state of Maryland to conduct an independent, third-party assessment of their cybersecurity practices at least every other year against the NIST Cybersecurity Framework. The results of these assessments would then be sent to the PSC and the Office of Security Management for their review and remediation through the PSC's workgroup process.

I want to thank the Maryland Cybersecurity Council and its Critical Infrastructure Subcommittee for their partnership in developing this bill. As threats to our systems continue to grow, so too must our capacity to prevent and mitigate them. **For these reasons, I respectfully request a favorable report on SB800.**

Sincerely,



Senator Katie Fry Hester
Howard & Montgomery Counties