Terri Jo Hayes
Executive Consultant, Cybersecurity Strategy and Policy, Mfusion, Inc.

Testimony in Support of

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

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

EXECUTIVE SUMMARY

Honorable Chair and members of the committee, thank you for the opportunity to provide testimony in support of Senate Bill 800 pertaining to cybersecurity and the Maryland Public Service Commission (PSC).

My name is Terri Jo Hayes. I have over 30 years of combined engineering and management, technology, and cybersecurity consulting experience, with over 15 years focused on critical infrastructure protection and cybersecurity operations and policy; and I serve as a member of the Maryland Cybersecurity Council.

Maryland is referred to as the Cyber Capital of America, the Hub of Cybersecurity Innovation. In 2019, the U.S. News and World reported[1] that there are more trained cyberengineers in Maryland than in the rest of the U.S. combined. While these are admirable characteristics for our State, these will just be statistics unless we can put the State's robust cybersecurity knowhow into action towards helping our increasingly vulnerable critical infrastructure become more cyber secure. I support the "Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)," SB800, because it places action behind our State as the Cyber Capital of America. It will establish an improved infrastructure that includes resources, technologies, and processes to help us become more intentional and proactive in protecting our most critical assets and provide a formal mechanism for reporting sector-wide cybersecurity posture to State Officials.

The Challenge

The aging U.S. electric grid is increasingly vulnerable as utility companies pursue efficiencies and cost savings through integration, modernization, and

[1] Janke, "Why Maryland is Home to Cyber Innovation," page 1.

digitization. While these modifications enhance the functionality and efficiency of the grid, they also increase their digital footprint for nefarious cyber actors to access and exploit. The Government Accountability Office (GAO) has been studying this environment and providing recommendations to address the increasing vulnerabilities and growing threat. GAO studies in 2019[2], 2021[3] and 2023[4] all state that the nation's grid is becoming more vulnerable to cyberattacks—particularly those involving industrial control systems (ICS) that support grid operations. In the recently published 2023 study, GAO reports that the U.S. grid's distribution systems remain increasingly at risk and need to be urgently addressed.

Some industry experts claim that the U.S. energy grid is completely interconnected, and our major worry is always the cascading failure scenario that would take down the entire grid. In addition, a majority of critical infrastructure, including financial services, communications, healthcare, and water systems rely on the electric grid for operation. Today, our infrastructures are integrated, connected, and dependent such that severe damage to the electric grid can cascade to other critical infrastructures. This integration was done out of efficiency and in some cases necessity. However, the integration comes with risks that have only grown as our systems expand and technology improves.

We have partners in this fight. The White House released the President's National Cybersecurity Strategy in March 2023, highlighting the importance of cybersecurity to the operation of our critical infrastructure. Furthermore, it encourages states that have authorities that can be used to set cybersecurity requirements to use them to enhance protection of our critical infrastructure.

Why I Support SB800

I support the passing of SB800 because it will help Maryland improve the cybersecurity of its increasingly vulnerable critical infrastructure. SB800 helps to proactively raise the bar of cybersecurity defenses by improving processes and structures at the PSC and utility companies, so that State Officials can have better awareness of the current cybersecurity posture of the electric, gas, and water utilities in Maryland. PSC understands the importance of critical infrastructure cybersecurity and has taken steps to bring a focus to addressing cybersecurity for its utilities. However, more rigor and

[2] U.S. Government Accountability Office, "Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid", Aug 2019

[3] U.S. Government Accountability Office," Electricity Grid Cybersecurity – DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems, March 2021

[4] U.S. Government Accounting Office, "Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure, February 2023

comprehensive practices are needed. For utilities, this Bill provides baseline protection of the infrastructure within a more formalized program, building upon the processes that are currently in place at the PSC. It provides a consistent framework that all utilities adhere to, not just those that have 30,000 or more customers. The framework may be resized for smaller utilities, who also need to implement robust cybersecurity practices. Information sharing may be challenging initially because of the culture and traditional barriers to sharing; but when implemented, it will help us better understand and address threats, and potentially avoid cyber attacks.

This Bill calls for establishing minimum security standards for each operational technology (OT) and information technology (IT) device, which requires utilities to inventory and baseline their systems, to understand the interconnections between IT and OT and the vulnerabilities that result. This process allows utilities to establish well-informed risk management plans and addresses CISA's best practices of identifying, minimizing, and securing all network connections to ICS assets.

The Zero Trust provisions is another feature of SB800 I fully support. The core principle behind Zero Trust is 'never trust, always verify'. Incorporating Zero Trust will significantly support a stronger defense, protecting IT/OT systems and stakeholder privacy information, and make it more challenging for an attacker to gain system access. It will help to establish the resiliency needed in our critical systems across the grid. This component of the Bill aligns with the Federal Government's Executive Order on Improving the Nation's Cybersecurity, which calls for agency heads to develop plans to implement a Zero Trust Architecture.

SB800 helps bring state legislation in better alignment with Federal priorities.

Amendments That Would Strengthen SB800

Two suggested amendments deal with information sharing and handling since such duties are key elements to most cybersecurity programs. The first amendment would recommend that certain classes of information and data shared by utilities under SB800 be given the protections provided by the Critical Energy Infrastructure Information (CEII) classification label and handled accordingly. CEII includes information about the production, transmission, or distribution of energy. In addition, any information that could be useful in planning an attack on critical infrastructure is considered CEII. According to the National Governor's Association, 28 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).[5]

The second amendment would recommend that the Commission staff responsible for handling utility cybersecurity assessment information hold a Top Secret clearance. Granting clearances to the appropriate members and staff enables better information sharing within the state government and amongst similarly cleared personnel throughout the federal government.

The final amendment is regarding timelines for public service company implementation activities. Providing timeline guidance in SB800 for public service company implementation may help clarify when such activities should begin or occur.

Cyber threats and vulnerabilities are growing in number and sophistication and will continue to be a threat to the electric grid and every other portion of our critical infrastructure. Though it will take time to reduce the risk, it is now clear to most that action must be taken at all levels of government and society to keep our country and State safe from the effects of cyber attacks on our critical infrastructure. I believe SB800 is a step in the right direction.

[5] National Governor's Association (NGA), "State Protection of Critical Energy Infrastructure Information (CEII)", https://www.nga.org/wp-content/uploads/2019/05/CEII-Paper-June-2019-Revised.pdf