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 SB 825 - Public Safety - Critical Infrastructure Protection**

March 3, 2026

Chair Feldman, Vice Chair Kagan, and members of the Education, Energy, and Environment Committee:

Thank you for your consideration of Senate Bill 825, which establishes a Critical Infrastructure Protection Branch within the Maryland Coordination and Analysis Center (MCAC) and creates clear, statewide measures to protect Maryland's critical infrastructure from cyber and physical threats.

Recent unclassified threat briefings make clear that modern adversaries increasingly seek to disrupt essential systems rather than rely on traditional physical attacks. Energy, water, transportation, communications, and food systems are now primary targets because disruption can create widespread economic and social instability without a single kinetic strike. Lessons from cyber operations observed in Ukraine and rising geopolitical tensions in the Indo-Pacific demonstrate that these threats are no longer hypothetical. Nation-state actors are actively probing U.S. infrastructure networks through persistent low-level intrusions designed to test vulnerabilities and maintain access.

As the traditional separation between information technology and operational technology disappears, physical infrastructure is increasingly exposed to foreign cyber intrusion. Recent examples include:

- Water & Energy — The FBI, NSA, and CISA have warned that Volt Typhoon, a state-sponsored Chinese hacker group, has already compromised the IT environments of multiple energy and water organizations as part of an effort to pre-position themselves on critical IT networks in the case of future crisis or conflict with the United States.[1]
- Transportation — In 2025, the Rhysida ransomware group claimed responsibility for breaching the Maryland Transit Administration's network and demanded $3.4 million,

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

causing system outages that affected customer-facing platforms and internal operations and requiring the agency to shift to manual processes during recovery.[2]

- Telecommunications — In late 2024, the state-sponsored Chinese hacker group Salt Typhoon infiltrated multiple U.S. telecommunication companies, including internet service providers.[3] Federal authorities report that this may have been an effort to gain access to communications between then-presidential candidates Kamala Harris, J.D. Vance, and Donald Trump.[4]
- Healthcare — Iranian government-sponsored cyber actors targeted Boston Children's Hospital in a "despicable" attempt to disrupt patient care, as characterized by FBI Director Christopher Wray.[5]

Last year, this Committee strengthened cybersecurity protections for Maryland's water systems through Senate Bill 871. However, protecting individual sectors alone is no longer sufficient. Maryland must adopt a comprehensive, statewide strategy that recognizes the interdependence of critical infrastructure systems.

During the interim, I participated in Colorado's Interlock Critical Infrastructure Briefing, where state leaders described how fragmented oversight limited preparedness. Colorado responded by creating a whole-of-state partnership uniting federal agencies, state government, the National Guard, law enforcement, and private-sector operators. Their model maintains a centralized infrastructure database, conducts regular cross-sector exercises, and validates contingency plans through ongoing coordination. They have also mapped infrastructure interdependencies, recognizing that disruption in one system—such as electric power—can cascade into failures across water treatment, healthcare delivery, communications, and transportation networks.

After returning to Maryland, I found that while many agencies are doing strong work within their missions, the State lacks a comprehensive framework integrating federal, state, and local partners. Maryland needs the ability to assess cyber threats alongside potential physical impacts, understand cross-sector dependencies, and coordinate planning and response before a crisis occurs.

SB 825 addresses this gap. Developed in collaboration with the Department of Homeland Security, the Maryland Department of Emergency Management, and the National Guard, the bill establishes a Critical Infrastructure Protection Branch within MCAC to coordinate agencies responsible for overseeing critical infrastructure statewide.

---

2 https://industrialcyber.co/transport/rhysida-ransomware-gang-claims-maryland-transit-administration-breach-demands-3-4-million/

3 https://www.congress.gov/crs-product/IF12798

4 https://www.cbsnews.com/news/trump-vance-potential-targets-china-backed-hacking-operation/

5 https://www.cbsnews.com/boston/news/boston-childrens-hospital-cyberattack-iran-indictments/

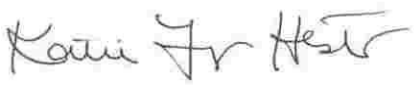
The Branch is charged with:

1. Analyzing potential threats and prioritizing critical infrastructure assets, including understanding vulnerabilities that could arise in the event of an attack;
2. Strengthening critical infrastructure assets within the State that are identified as priorities;
3. Working with the Maryland Department of Emergency Management (MDEM) to map cascading impacts of an attack on critical infrastructure and create response plans;
4. Working with the Department of Information Technology (DoIT) to provide up-to-date cybersecurity reporting standards to owners and operators of critical infrastructure;
5. Collaborating with MDEM to respond to attacks if they happen;
6. Coordinating with the Governor's Office of Homeland Security and critical industry, local, and federal counterparts on issues pertaining to critical infrastructure.

SB825 ensures Maryland is prepared to confront evolving threats. Our critical infrastructure provides essential services including healthcare, communications, and water access. Maryland residents and agencies have already experienced the consequences of cyber disruptions. This legislation positions the State to be proactive rather than reactive.

For these reasons, I respectfully request a favorable report on SB825.

Sincerely,



Senator Katie Fry Hester
Howard and Montgomery Counties