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 SB183 - Public Safety - Maryland Cyber Reserve - Established

February 10, 2026

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

Thank you for your consideration of SB183, which establishes the Maryland Cyber Reserve within the Military Department to ensure that the State has a ready body of cybersecurity experts to provide rapid response assistance in the event of a cyberattack.

Nationally, cyberattacks are becoming more frequent and sophisticated—particularly with the use of artificial intelligence—and have already disrupted essential services and imposed significant costs on the State. In just one year, from 2024-2025, ransomware incidents in the US rose by roughly 146%, and the US accounted for about 50% of ransomware attacks worldwide.[1] Further, U.S. cybercrime costs have grown from about $19.4 billion in 2023 to $639.2 billion in 2025.[2]

As Maryland's critical infrastructure increasingly relies on digital systems, cybersecurity threats pose a direct risk to public safety, service delivery, and fiscal stability. Cyber attacks are becoming more frequent and sophisticated and have already disrupted essential services and imposed significant costs on the State, for example:

- Frederick Health Medical Group (April 2024): A ransomware attack compromised the sensitive personal and medical information of more than 934,000 patients.[3]

---

1 https://www.techradar.com/pro/security/us-becomes-ransomware-capital-of-the-world-as-attacks-rise-by-almost-150-percent/

2 https://cyberzoni.com/stats/estimated-us-cybercrime-cost/

3 https://www.hipaajournal.com/frederick-health-medical-group-ransomware-attack/

- Maryland Department of Health (2022): A cyberattack disrupted COVID-19 data reporting and prevented residents from applying for Medicaid, limiting access to essential health services.[4]
- Anne Arundel County Government (February 2025): An intrusion into county systems allowed unauthorized access to sensitive data, including confidential Department of Health information.[5]
- Baltimore County Public Schools (2023): A cyberattack resulted in nearly $10 million in recovery and remediation costs to the State.[6]

Unfortunately, at the same time attacks are going up, federal support for state and local cybersecurity has declined, leaving states to shoulder more responsibility for protecting critical infrastructure and public systems. The State and Local Cybersecurity Grant Program (SLCGP) has expired, and its reauthorization is stalled in Congress. The Cybersecurity and Infrastructure Security Agency (CISA) have shifted away from longstanding cooperative agreements with organizations like the Multi-State Information Sharing and Analysis Center (MS-ISAC), which has historically provided free or low-cost threat intelligence and incident response services to states and local governments. These trends — declining grant allocations and reduced direct operational support — coincide with rising cyber threats to state systems, underscoring the need for Maryland and other states to bolster their own cyber workforce, resiliency planning, and operational capabilities to ensure continuity of government services and protect sensitive data.

Maryland has made meaningful progress in strengthening our cybersecurity posture. Since this committee passed the Cybersecurity Governance Act of 2022, staffing at the Maryland Office of Security Management has grown from just four full-time employees to thirty-four. We have also added dedicated cybersecurity expertise at the Public Service Commission and an operational technology expert at the Department of Information Technology. Even with this growth, the State cannot afford to hire and retain enough full-time personnel to meet the scale and speed of today's threats. SB183 offers a cost-effective solution by tapping into one of Maryland's greatest assets: the thousands of highly trained cybersecurity professionals in our private sector who are eager to serve and volunteer their expertise when the State needs them most.

---

4 https://www.hipaajournal.com/disruption-to-maryland-department-of-health-services-continues-one-month-after-ransomware-attack/

5 https://www.aacounty.org/cyber-incident

6 https://abcnews.com/US/baltimore-schools-failed-fully-act-security-recommendations-cyber/story?id=96671802

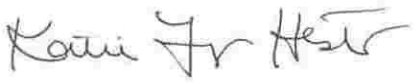
SB183 addresses the threat of cyberattacks in several ways, borrowing from a framework already successful in Michigan,[7] Ohio,[8] and Texas.[9] The establishment of a Cyber Reserve would assist the State by ensuring a ready group of cybersecurity experts is accessible in the event of a cyber emergency, mobilizing the expertise already within Maryland to more effectively protect State interests. Specifically, the bill:

- Establishes the Maryland Cyber Reserve within the Military Department as a new component of the State's organized militia, composed of both commissioned Officers and a volunteer force of qualified professionals;
- Places the Cyber Reserve under the authority of the Governor as Commander-in-Chief, and under the operational control of the Adjutant General;
- Authorizes the Cyber Reserve to provide educational and technical support to respond to cyberattacks targeting the State, counties, local agencies, and critical infrastructure within Maryland; and
- Permits deployment to assist Maryland corporations and citizens affected by cyberattacks when directed by competent authority.

This legislation was developed using models established by several other States invested in improving cybersecurity. In a world where waterways are managed through a computer system, the value of ready cyber expertise cannot be understated. By establishing a Cyber Reserve, our State can ensure that cyberattacks can be responded to effectively, efficiently, and appropriately, protecting Maryland's security and residents' safety.

For these reasons, I respectfully request a favorable report on SB183.

Sincerely,



Senator Katie Fry Hester
Howard and Montgomery Counties

---

[7] https://law.justia.com/codes/michigan/2020/chapter-18/statute-act-132-of-2017/section-18-223-amended/

[8] https://codes.ohio.gov/ohio-revised-code/section-5922.01/1-24-2020#:~:text=Section%205922.01%20%7C%20Creation.&text=In%20the%20case%20of%20an,exigency%20of%20the%20occasion%20requires.

[9] https://sn.lexisnexis.com/opentext/eyJ0eXBlIjoiYmlsbCIsImlkIjoiVFgyMDI1MDAwSDE1MCJ9.VwlX-MXRwSaIH-3JspcwQQoMJDyckeWtGEva6oFNN5A/text