SB 183
Uploaded by: Christian Djachechi
Position: FAV

The Maryland Cyber Reserve

- A Force Multiplier for State-Wide Protection

About Our Company

No Jurisdiction Left Behind:

Democratizing High-End Cyber Defense.

Culture of Innovation

Operationalizing NIST: From Framework to Frontline Protection."

Ethics and Sustainability

We are committed to sustainable and ethical practices, aiming to positively impact our industry and communities.

The Value Of Innovation

New Advanced Technologies

GLOBAL ASSET DEVELOPMENT GROUP LLC

The Problem – Uneven Capacity

A Digital Divide in Defense

- **Critical Dependence:** Maryland's elections, public safety, schools, and water systems depend entirely on digital infrastructure.
- **Real Threats:** Ransomware and cyberattacks on schools and water plants have already disrupted services and cost taxpayers millions.
- **The Gap:** While large state agencies have dedicated teams, small counties and municipalities cannot afford 24/7 monitoring or full-time cyber professionals.
- Implementation Struggle: Frameworks like NIST exist, but jurisdictions outside of Annapolis lack the personnel to execute them.

The Solution – Senate Bill 183

- **Organizational Structure:** Creates the Maryland Cyber Reserve within the Military Department as part of the organized militia.
- **Core Mission**: Provide technical support to prevent and resolve cyberattacks for government agencies, businesses, and private citizens.
- **Why This Design Works:**
  - Emergency Status: Explicitly adds cyberattacks as a trigger for militia activation, similar to natural disasters.
  - Ready Cadre: Maintains a standing pool of trained officers and volunteers.
  - Cost-Effective: Members serve without pay unless activated, keeping baseline costs low.

Operationalizing NIST Standards

Bridging the implementation gap: Moving from high-level mandates to field-level actions.

Actionable Support:

- Conducting NIST-aligned risk assessments and remediation plans for local governments.
- Deploying standardized playbooks for incident response and threat hunting.
- Using advanced tools like Zero Trust Network Access and SOAR automation to reduce response times.
- Assisting with "Authorization to Operate" (ATO) so small entities don't have to "reinvent the wheel".

Protecting Maryland Businesses & Citizens

- **Direct Assistance**: SB0183 allows the Reserve to help corporations and individual citizens targeted by attacks.
- **First Responder Guidance:** Offering standardized triage for ransomware and account takeovers.
- **Community Resilience:** Delivering tabletop exercises and education for small businesses and nonprofits.
- **Navigational Aid:** Coordinating with existing reporting mechanisms so citizens are not left alone during a crisis.

Governance, Ethics, & Trust

Ethical Safeguards: Regulations will prohibit members from accepting certain compensation or benefits to prevent conflicts of interest or vendor steering.

Accountability: Being situated in the Military Department ensures strict discipline, readiness metrics, and after-action reviews.

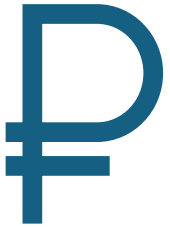
Long-Term Workforce Strategy

- **Talent Pipeline:** Engaging students, veterans, and professionals in real-world missions.
- **Partnerships:** Linking the Reserve with universities and K–12 programs to provide practicum-style experience.
- **Outcome:** Building a larger pool of cyber talent that stays in Maryland.

Conclusion & Call to Action

Closing Argument: Existing laws set the direction, but SB0183 provides the "hands and brains" to do the work.

Goal: Ensuring every small town has access to enterprise-grade cyber defense.



Recommendation: A favorable report for SB0183.

SB183_Oral_Testimony_Committee_Submission_FINAL_Wi
Uploaded by: Donna DiMichele
Position: FAV

Oral Testimony Submission – Senate Bill 183

Maryland Senate Education, Energy, and the Environment Committee
Bill Hearing: February 12, 2026
Submitted: February 10, 2026
Position: Favorable

Chairman Feldman, Vice Chair Kagan, and Members of the Committee:

Thank you for the opportunity to testify today in support of Senate Bill 183, legislation establishing the Maryland Cyber Reserve.

My name is Nicklous Combs. I am Chairman and Chief Executive Officer of FGS LLC, a Maryland-based company that supports the missions of the Department of Defense, the Intelligence Community, and law enforcement organizations.

I began my career as a cryptologic technician supporting the National Security Agency and went on to serve across the U.S. Army, the Intelligence Community, and the private sector, including in senior executive roles as a Chief Information Officer and Chief Technology Officer.

Across more than four decades of service, one lesson has remained constant: technology matters—but people matter more. In a real cyber incident, success depends on whether trusted, experienced professionals are ready to respond immediately.

While artificial intelligence delivers enormous benefits, it is not something we can put back in the box. Human behavior remains the weakest link in cybersecurity, and artificial intelligence now weaponizes that weakness—enabling individual bad actors to do what, until recently, only nation-state actors could accomplish.

Attacks can now be launched faster, at greater scale, and with far less warning, overwhelming traditional defenses and response models.

Artificial intelligence has permanently changed the cybersecurity threat landscape. There is no reset button. AI is embedded in how Maryland educates its students, delivers power, manages water, and protects the environment. The only question before us is whether the

State is prepared for the risks that come with that reality.

For Maryland, this carries unique risk. Our State sits at the center of the nation's cyber ecosystem and is home to federal agencies, defense contractors, research universities, healthcare systems, ports, and critical infrastructure. The same concentration of talent and data that powers our economy also makes Maryland a high-value target for sophisticated adversaries.

Cyberattacks are no longer theoretical, and preparedness is no longer optional. If education systems go down, learning stops. If energy systems are disrupted, public safety is at risk. If water systems are compromised, the consequences are immediate and real. These are not abstract cyber events—they are operational failures with real-world impact.

That same human vulnerability, now amplified by artificial intelligence, is why preparedness and rapid response matter.

Cybersecurity is no longer just an IT problem. It is a public safety issue, an economic resilience issue, and a governance issue that cuts across every responsibility of this Committee.

No single agency, school system, or utility can maintain all the expertise needed to defend against these threats on its own. When incidents escalate, what matters is speed, coordination, and access to experienced professionals. Preparedness—not perfection—is what determines outcomes.

Cybersecurity is a team sport. Senate Bill 183 recognizes that cyber incidents are inevitable, but being unprepared is not. The Maryland Cyber Reserve provides the State with a disciplined, practical mechanism to rapidly surge skilled professionals, train and plan in advance, and coordinate effectively across government and the private sector—before a crisis occurs, not after.

Cyber Reserve allows Maryland to rapidly mobilize trusted expertise to protect public services, critical infrastructure, and public trust.

Maryland has extraordinary cyber talent. This bill provides a responsible and effective way to organize that talent in service of the State when it is needed most.

I would like to thank Senator Katie Fry Hester for her leadership and foresight in advancing this legislation.

I respectfully urge the Committee to give Senate Bill 183 a favorable report.

Thank you for your time and consideration.

Nicklous “Nick” Combs
Chairman and Chief Executive Officer
FGS LLC

SB183_Written_Testimony_Nicklous_Combs_Final.pdf
Uploaded by: Donna DiMichele
Position: FAV

Written Testimony – Senate Bill 183

Maryland Cyber Reserve

Maryland Senate Education, Energy, and the Environment Committee
Bill Hearing: February 12, 2026
Submitted: February 10, 2026

Chairman Feldman, Vice Chair Kagan, and Members of the Committee:

Thank you for the opportunity to submit written testimony in support of Senate Bill 183, legislation that establishes the Maryland Cyber Reserve.

My name is Nicklous Combs. I am Chairman and Chief Executive Officer of FGS LLC, a Maryland-based company that supports the missions of the Department of Defense, the Intelligence Community, and law enforcement organizations. I began my career as a cryptologic technician supporting the National Security Agency and went on to serve across the U.S. Army, the Intelligence Community, and the private sector, including in senior executive roles as a Chief Information Officer and Chief Technology Officer.

Across more than four decades of service, one lesson has remained constant: technology matters, but people matter more. In a real cyber incident, success depends on whether trusted, experienced professionals are ready to respond immediately.

While artificial intelligence delivers enormous benefits, it is not something we can put back in the box. Human behavior remains the weakest link in cybersecurity, and AI is now enabling individual bad actors to do what, until recently, only nation-state actors could accomplish. Attacks can now be launched faster, at greater scale, and with far less warning, overwhelming traditional defenses and response models.

Artificial intelligence has permanently changed the cybersecurity threat landscape. There is no reset button. AI is embedded in how Maryland educates its students, delivers power, manages water, and protects the environment. The only question before us is whether the State is prepared for the risks that come with that reality.

For Maryland, this carries unique risk. Our State sits at the center of the nation's cyber ecosystem. We are home to federal agencies, defense contractors, research universities, healthcare systems, ports, and critical infrastructure. The same concentration of talent and

data that powers our economy also makes Maryland a high-value target for sophisticated adversaries.

Cyberattacks are no longer theoretical, and preparedness is no longer optional. If education systems go down, learning stops. If energy systems are disrupted, public safety is at risk. If water or environmental control systems are compromised, the consequences are immediate and real. These are not abstract cyber events—they are operational failures with real-world impact.

For decades, we have known a simple truth: human behavior is the weakest link in cybersecurity. Artificial intelligence does not fix that weakness—it weaponizes it. Today, a single individual using AI-enabled tools can execute cyber operations that once required the time, money, and manpower of a nation-state. That shift is happening now, and it directly affects Maryland.

Cybersecurity is no longer an IT problem. It is a public safety issue. It is an economic resilience issue. And it is a governance issue that cuts across every responsibility of this Committee.

No single agency, school system, or utility can maintain all the expertise needed to defend against these threats on its own. When incidents escalate, what matters is speed, coordination, and access to experienced professionals. Preparedness—not perfection—is what determines outcomes.

Cybersecurity is a team sport. Senate Bill 183 recognizes that cyber incidents are inevitable, but being unprepared is not. The creation of a Maryland Cyber Reserve provides the State with a disciplined, practical mechanism to rapidly surge skilled professionals, train and plan in advance, and coordinate effectively across government and the private sector—before a crisis occurs, not after.

A Cyber Reserve allows Maryland to rapidly mobilize trusted expertise to protect public services, critical infrastructure, and public trust. It strengthens resilience, shortens response time, and ensures continuity of essential services when they are needed most.

Maryland has extraordinary cyber talent. Senate Bill 183 provides a responsible and effective way to organize that talent in service of the State during times of need. Passing this bill sends a clear signal that Maryland understands the modern cyber threat, accepts its reality, and is prepared to defend its people, its economy, and its mission.

I would like to thank Senator Katie Fry Hester for her leadership and foresight in advancing this legislation. I respectfully urge the Committee to give Senate Bill 183 a favorable report.

Thank you for your time and consideration.

Respectfully submitted,

Nicklous “Nick” Combs
Chairman and Chief Executive Officer
FGS LLC

SB0183_MACC_FAV.pdf
Uploaded by: Drew Jabin
Position: FAV

MACC
MARYLAND ASSOCIATION OF COMMUNITY COLLEGES

60 West Street, Suite 200
Annapolis, MD 21401
410-974-8117

Senate Education, Energy, and the Environment Committee
February 12, 2026

SB 183 - Public Safety - Maryland Cyber Reserve - Established

Position: Favorable

The Maryland Association of Community Colleges (MACC), representing Maryland's 16 community colleges, supports **SB 183**, which establishes the Maryland Cyber Reserve within the Military Department to strengthen the State's capacity to prevent and respond to cyber attacks. As cyber threats continue to grow in frequency and sophistication, Maryland must build a resilient, skilled, and mission-ready cybersecurity workforce capable of supporting State and local governments and critical infrastructure.

Maryland's community colleges play a central role in developing the State's cybersecurity talent pipeline. Through affordable, accessible, and industry-aligned programs, community colleges train thousands of students each year in cybersecurity, networking, and related technical fields. These programs serve both traditional students and working adults seeking to upskill or transition into cybersecurity careers, making community colleges uniquely positioned to support a reserve-based cyber response model that relies on trained professionals who can be activated as needed. In particular, MACC's Cyber Workforce Accelerator demonstrates how community colleges can operate at scale to meet Maryland's cybersecurity workforce needs. The Accelerator connects community colleges, employers, and public partners to deliver coordinated training, credentialing, and workforce pathways aligned with real-world cyber defense needs. Senate Bill 183 complements this existing infrastructure by creating a formal mechanism for trained cybersecurity professionals, including those educated through community college programs, to serve the State in times of need while continuing their civilian careers.

By establishing the Maryland Cyber Reserve, the State recognizes cybersecurity as a core component of public safety and emergency preparedness. Leveraging community college-led training initiatives and workforce partnerships will be critical to the long-term success of the Reserve and to ensuring that Maryland has a deep, diverse, and geographically distributed pool of cyber talent ready to respond to emerging threats. Accordingly, MACC urges the Committee to issue a **FAVORABLE** report on **SB 183**.

Please contact Brad Phillips (bphillips@mdacc.org) or Drew Jabin (djabin@mdacc.org) with questions.

MML- FAV- SB 183.pdf
Uploaded by: Iris Ibegbulem
Position: FAV

TESTIMONY

COMMITTEE:	Senate Education, Energy, and the Environment	**DATE:**	February 12, 2026
POSITION:	Favorable	**BILL:**	SB 183

The Maryland Municipal League (MML) supports House Bill 183.

House Bill 183 aims to provide educational and technical support which would prevent and resolve cyber-attacks against State, county, and local government agencies. Under the bill, local governments and municipalities would be able to receive increased state-supported cybersecurity protection, education, and incident response.

Considering half of the municipalities within our membership have less than 10 paid employees and far less have staff with cybersecurity expertise, having the Maryland Cyber Reserve to act on cyber threats allows for faster, competent responses in case of a crisis. Giving municipalities across the state access to skilled, professional assistance also improves equity for under-resourced areas across the state.

By shifting cybersecurity incidents from a local or municipal concern to a shared State responsibility, this allows for better and faster recovery. Furthermore, timely responses and effective recovery can reduce the likelihood of extended outages, decrease data loss, and strengthen municipal public trust.

For these reasons, the League respectfully requests that the committee provide Senate Bill 183 with a favorable report.

For more information relating to this piece of testimony, please contact:

Iris Ibegbulem: Manager, Advocacy and Public Policy, irisi@mdmunicipal.org

SB183 Testimony Hester.pdf
Uploaded by: Katie Fry Hester
Position: FAV

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

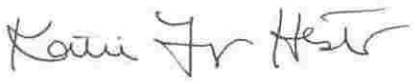
SB183 addresses the threat of cyberattacks in several ways, borrowing from a framework already successful in Michigan,[7] Ohio,[8] and Texas.[9] The establishment of a Cyber Reserve would assist the State by ensuring a ready group of cybersecurity experts is accessible in the event of a cyber emergency, 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

SB183_FAV_Rolfe.pdf
Uploaded by: Nathan Rolfe
Position: FAV

February 12, 2026

Nathan Rolfe
Woodbine, MD 21797

TESTIMONY ON SB 183 - POSITION: FAVORABLE
Public Safety – Maryland Cyber Reserve – Established

TO: Chair, Vice Chair, and members of the Education, Energy, and the Environment Committee
FROM: Nathan Rolfe, President, Association of U.S. Cyber Forces (AUSCF)

My name is Nathan Rolfe. I am submitting this testimony in support of SB 183, Public Safety – Maryland Cyber Reserve – Established. This is submitted both as a private resident of Maryland's District 9, and as organizational support on behalf of AUSCF.

Maryland stands at a critical juncture regarding its digital infrastructure. Establishing the Maryland Cyber Reserve (MCR) is a forward-thinking solution that provides the State with the necessary agility to deploy talent and technical capabilities precisely when and where they are needed during a cyber incident. This initiative creates a vital safety net for our state and local agencies, ensuring we are not left vulnerable to evolving digital threats.

To ensure the MCR is a hub for true innovation, I strongly advocate for a recruitment strategy that prioritizes skills-based assessments over traditional educational degrees or basic industry certifications. The cybersecurity field is filled with 'specially qualified' individuals who have achieved high-level expertise through non-traditional means. By focusing on demonstrable ability, the State can tap into a broader, more capable talent pool that traditional hiring processes often overlook.

Furthermore, the selection of senior leadership within the MCR must be handled with precision. Effective command of a reserve force during a crisis requires more than just technical skill or a C-suite title at a technology firm; it requires deep experience in the planning and execution of military cyberspace operations. Prioritizing leaders who understand operational coordination and mission-critical strategy within a militia structure is essential for the Reserve's success.

Finally, the Maryland Cyber Reserve offers a powerful alternative to traditional schooling for workforce development. By providing a venue for 'hands-on' experience with relevant, real-world cyber incidents, the MCR will grow a world-class talent pool within Maryland. This practical experience is invaluable for both the individual members and the State's overall economic and security posture.

Passing this bill will fix a critical gap in our defensive posture while simultaneously building a premier talent pipeline for the future. I respectfully urge this committee to return a favorable report on SB 183.

Respectfully submitted,

Nathan Rolfe

SB0183-EEE_MACo_SWA.pdf
Uploaded by: Charlotte Fleckenstein
Position: FWA

Senate Bill 183

Public Safety - Maryland Cyber Reserve - Established

MACo Position: **SUPPORT WITH AMENDMENTS**

To: Education, Energy, and the Environment Committee

Date: February 12, 2026

From: Karrington Anderson and Charlotte Fleckenstein

The Maryland Association of Counties (MACo) **SUPPORTS** SB 183 **WITH AMENDMENTS**. This bill establishes the Maryland Cyber Reserve within the Military Department to provide educational and technical support to help prevent and respond to cyberattacks affecting state, county, and local government agencies, as well as critical infrastructure across Maryland.

Counties support the bill's goal of leveraging cybersecurity expertise to strengthen preparedness and response capabilities. Local governments are frequent targets of increasingly sophisticated cyber threats, and SB 183 represents a positive step toward enhancing statewide coordination and resilience. To ensure clear and effective implementation, MACo requests several clarifying amendments related to county participation and operational coordination.

MACo's amendments focus on clarifying how the Maryland Cyber Reserve would engage with counties in practice. Specifically, the bill would benefit from clearer language regarding county consent, authorization for access to county systems and data, appropriate data protections, and the parameters governing the start and conclusion of Maryland Cyber Reserve assistance. These clarifications would help ensure effective coordination while preserving existing local governance structures.

Ensuring that assistance is voluntary, subject to county authorization, and governed by clear data protections and agreed-upon activation and deactivation criteria would preserve local authority while ensuring effective collaboration. With these clarifications, SB 183 can serve as a valuable and trusted resource for counties during cyber incidents.

For these reasons, MACo urges a **FAVORABLE WITH AMENDMENTS** report on SB 183 *(MACo's suggested "local option" amendment language is included on the next page).*

MACo Amendments on SB 183:

On page 4, in line 18, after "**(2)**" insert "**ANY TECHNICAL SUPPORT PROVIDED TO THE COUNTY, OR LOCAL GOVERNMENT AGENCY SHALL BE AT THE REQUEST OR APPROVAL OF THE COUNTY, OR LOCAL GOVERNMENT.**

(3) THE MARYLAND CYBER RESERVE SHALL OBTAIN AUTHORIZATION FROM A LOCAL GOVERNMENT CHIEF INFORMATION SECURITY OFFICER, A COUNTY OR CITY ADMINISTRATOR, OR EQUIVALENT TO ACCESS THE LOCAL GOVERNMENT SYSTEM.

(4) ALL INFORMATION ACCESSED OR GENERATED BY THE MARYLAND CYBER RESERVE WHILE ASSISTING A COUNTY OR LOCAL GOVERNMENT ENTITY SHALL BE SUBJECT TO APPLICABLE CONFIDENTIALITY, RECORDS RETENTION, AND DATA PROTECTION LAWS, AND SHALL REMAIN THE PROPERTY OF THE COUNTY OR LOCAL GOVERNMENT ENTITY.

(5) ASSISTANCE PROVIDED TO A COUNTY OR LOCAL GOVERNMENT ENTITY SHALL BE GOVERNED BY WRITTEN ACTIVATION AND DEACTIVATION CRITERIA AGREED UPON BY THE MARYLAND CYBER RESERVE AND THE COUNTY OR LOCAL GOVERNMENT ENTITY PRIOR TO ENGAGEMENT.

(6)".

SB 183 - Informational Testimony by the UC Berkele

Uploaded by: Sarah Powazek

Position: INFO

UC Berkeley CLTC Center for Long-Term Cybersecurity

Center for Long-Term Cybersecurity
University of California, Berkeley
102 South Hall #4600
Berkeley, CA 94720
https://cltc.berkeley.edu

Testimony on SB183: Public Safety - Maryland Cyber Reserve - Established

Committee: Education, Energy, & the Environment Committee Testimony on SB-0183
Position: Informational Only
Hearing Date: February 11, 2026

Good afternoon, Chairman Feldman, Vice Chair Kagan, and members of the Education, Energy, & the Environment Committee, and thank you for this opportunity to speak in an informational capacity about SB183 and the establishment of a Maryland Cyber Reserve.

The UC Berkeley Center for Long-Term Cybersecurity's (CLTC) works to help individuals and organizations address tomorrow's information security challenges and amplify the upside of the digital revolution. We cofounded and chair the Consortium of Cybersecurity Clinics, a collective of over 43 colleges and universities in the U.S., including University of Maryland, Baltimore County (UMBC), and over 57 worldwide that provide free cybersecurity risk assessments and recommendations to nonprofits, small critical infrastructure, fire departments, schools, cities, and towns.

CLTC is also the largest convener of cyber volunteering organizations in the country; we co-chair the Cyber Resilience Corps, which strengthens volunteer efforts to deliver real, hands-on cybersecurity support where it's needed most. We have a birds-eye view of these programs nationwide, and are currently tracking over 66 state, county, or city-based cyber defense programs. We regularly work with states to share best practices and improve the services and connectivity of cyber volunteering programs.

CLTC is focused on regional cyber capacity-building programs like these because community organizations often cannot afford to protect themselves against cyberattacks, which disrupt critical human services for residents. In fact, 34% of state and local governments experienced a ransomware attack in 2024[1], and there was a 70% increase in attacks on U.S. utilities from the same period in 2023 to 2024.[2] The ongoing cost of cybersecurity far exceeds the budgets available to most small organizations, which also often lack the in-house cyber expertise to protect themselves from cyberattacks.

Through CLTC's work, we have seen the **power of expert volunteers to fill critical gaps in cybersecurity** services nationwide:

- Cybersecurity clinics have served over 700 client organizations.
- As of May 2025, there are approximately 3,900 cyber volunteers in the U.S. spread across 50 volunteer groups serving around 500 client organizations per year.

Cyber reserve teams are no longer experimental or pilot programs; they follow well-trodden paths that have been in place for many years in several states. As of 2025, cyber reserve programs are operational in Michigan, Wisconsin, Texas, Ohio, Virginia, and Louisiana, and new programs are developing in Oklahoma, Washington, and New Jersey.

---

[1] 2024 Ransomware Report: Sophos State of Ransomware.
[2] Dareen, Seher and Vallari Srivastava. "Cyberattacks on US Utilities Surged 70% This Year, Says Check Point" | Reuters, 11 Sept. 2024.

UC Berkeley CLTC Center for Long-Term Cybersecurity

Center for Long-Term Cybersecurity
University of California, Berkeley
102 South Hall #4600
Berkeley, CA 94720
https://cltc.berkeley.edu

These cyber reserve programs typically provide both proactive (pre-incident) and reactive (post-incident) services, including: (1) education and training; (2) vulnerability and risk assessments; and (3) on-call expertise, incident response, and recovery efforts. These services in the private marketplace can cost in the tens of thousands of dollars, which is unaffordable for most small cities, towns, and utilities. Cyber reserve teams help ensure these public organizations get the assistance they could not otherwise afford.

In addition to serving the community, cyber reserve teams can provide several benefits to the states that run them, most notably by saving taxpayer money by reducing the costs of cybersecurity incidents to local governments and critical infrastructure. For example, **for every $1 spent on the Wisconsin Cyber Reserve Team (CRT), volunteers saved cyber victims $1.40** in costs such as incident response and recovery. These programs can also improve a state's cyber resilience by training critical infrastructure operators and remediating vulnerabilities, creating surge capacity in the event of a regional or statewide cyber emergency, and enhancing a state's cybersecurity workforce.

Cyber reserve teams can readily complement other established state cyber defense programs. A cyber reserve corps could coordinate with the Maryland Defense Force (MDDF) to ensure local governments receive the same standard of care as state agencies, as well as partner with MDEM's Cyber Preparedness Unit to expand the delivery of a range of services like cyber incident response training and rewriting emergency operations plans. A cyber reserve team could also recruit from the strong student pipeline at the cyber clinic at UMBC and the two clinics soon to be established through the Cyber and Artificial Intelligence (AI) Pilot Clinic Grant Initiative from the Maryland Department of Labor.

However, there are several hurdles that cyber reserve programs need to overcome, including managing liability, building trust with localities, and recruiting, vetting, and maintaining a corps of volunteers. Existing cyber reserve programs have addressed these in different ways, and CLTC would be glad to connect any Committee members to counterparts in other states to share their solutions.

We also want to highlight the role of civil society in providing essential human services like housing assistance, food access, youth development programs, and disaster relief. State and local governments regularly fund and contract with nonprofits as extensions of their public service delivery system to support vulnerable populations. Because of this role, nonprofits can be just as important to the health and well-being of residents as traditional critical infrastructure, and **civil society would be deserving beneficiaries** of cyber volunteering programs like cyber reserve teams.

Thank you again for this opportunity to share more information about regional cyber volunteering[3] and cyber capacity-building programs with the Committee.

The UC Berkeley CLTC | Public Interest Cybersecurity Program

Sarah Powazek — Director
Shannon Pierson — Senior Fellow
Grace Menna — Senior Fellow

[3] More information on the location of cyber volunteering programs can be found at cybervolunteers.us, on cyber clinics at cybersecurityclinics.org, and a broad overview of the state of cyber volunteering and recommendations for areas of improvement in our report "The Roadmap to Community Cyber Defense" at cltc.berkeley.edu.