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