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.

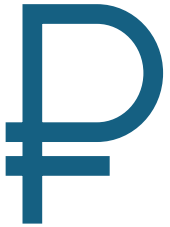
Long-Term Workforce Strategy

- **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.