Charles Harry, PhD
Director
Center for Governance of Technology and Systems
University of Maryland, College Park

SCHOOL OF PUBLIC POLICY
CENTER FOR GOVERNANCE OF TECHNOLOGY AND SYSTEMS

Position: Support

Thank you for the opportunity to submit this written testimony on behalf of SB 907/HB 1309. My name is Dr. Charles Harry, and I am a cybersecurity expert with 20 years of experience, a resident of a county recently affected by a cyberattack, and a father with a child in the Maryland Public School System. I am deeply concerned about the security of Maryland's educational institutions.

I serve as the Director of the Center for the Governance of Technology and Systems (GoTech) and as an Associate Research Professor at the University of Maryland, College Park. My center focuses on strategic cybersecurity and risk estimation across critical infrastructures. Prior to this role, I spent over 20 years in national security, including serving as a senior intelligence leader at the National Security Agency, where I specialized in cyber operations and supported critical national security concerns.

The Growing Cybersecurity Threat to Schools

Cyber threats targeting critical infrastructure are increasing in complexity and impact, particularly in public school districts. These institutions face sophisticated and financially motivated attacks designed to disrupt school networks and pressure public officials into paying ransoms to regain access to compromised systems. Between 2014 and September 2024, GoTech identified 425 cyber events in K-12 schools nationwide. This number likely underrepresents the true scope of the problem. Among these incidents:

- **97%** were perpetrated by criminal actors with financial motives.
- **71%** caused disruptions to critical school services, in some cases leading to lost classroom time lasting days.

In Maryland, recent cyberattacks have compromised both critical operations and student data confidentiality including the following events:

- **2023:** Prince George's County Public Schools experienced unauthorized access between August 3 and August 14 requiring the purchase of indemnity monitoring services.
- **2020:** Baltimore County Public Schools suffered a ransomware attack that cost over $10 million to remediate.
- **2016:** Frederick County Public Schools experienced a data breach affecting over 1,000 students.

How Attacks Occur

Cybercriminals exploit vulnerabilities in internet-facing devices, commonly referred to as the attack surface. They also use phishing emails and compromised passwords to infiltrate networks, allowing them to steal data or deploy ransomware, crippling critical school functions. The likelihood of these attacks

depends on the number of exposed devices and software vulnerabilities. This past weekend, GoTech conducted a strategic cybersecurity risk assessment of Maryland's county school systems using the same publicly available information that threat actors leverage. We identified a large and diverse attack surface, including:

- **451** internet-routable devices
- **1,399** open ports
- **768** software services
- **280** potential vulnerabilities
- **5** school systems with vulnerabilities that have a high probability of exploitation (>0.90 EPSS value)
- **4** school systems with known vulnerabilities listed on CISA's actively exploited vulnerability list

While this data is concerning, it is only part of the broader risk landscape. Many school networks also have compromised passwords actively traded on the dark web. In a previous analysis of county governments, GoTech identified multiple compromised credentials available for sale.

I will not discuss specific school systems in this testimony, but I am happy to share our findings with the appropriate county personnel to provide assistance if needed.

Why This Matters

Currently, individual school districts make cybersecurity decisions without systematic, continuous monitoring of their networks. These isolated decisions have broader consequences. A comprehensive, statewide approach to cybersecurity risk management is necessary.

Implementing a universal set of cybersecurity principles—aligned with national best practices such as those from the National Institute of Standards and Technology (NIST)—will help reduce risk. These principles form the foundation of Maryland's minimum cybersecurity standards and are essential for securing critical infrastructure. While concerns about the cost of implementing these security measures are valid, the financial and operational impact of large-scale cyber disruptions makes these investments both necessary and prudent.

Maryland's public schools play a vital role in our communities, and their security must be a priority. I urge the committee to support this bill and take proactive steps to strengthen cybersecurity across the state's school systems.

Thank you for your time and consideration.

Charles Harry, PhD
Director
Center for Governance of Technology and Systems
University of Maryland, College Park