OPEN DISTRICT
SOLUTIONS
Cybersecurity | Crisis Management | Resilience

Testimony in Support of Senate Bill 907: Enhancing the Cybersecurity Posture of Maryland's Local School Systems

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

I write to express my strong support for Senate Bill 907, which seeks to enhance the cybersecurity posture of Maryland's local school systems by mandating adherence to State Minimum Cybersecurity Standards (SMCS) and requiring biennial cybersecurity maturity assessments. Over the past two decades, I have served in public safety and cybersecurity roles—including having the honor and pleasure serving as the first Director of Local Cybersecurity for the State, six years in Montgomery County's Office of Emergency Management and Homeland Security, leading the County's cybersecurity resilience program, and now as President of Cybersecurity Strategy and Resilience at Open District Solutions. I have witnessed firsthand the critical importance of proactive cybersecurity measures in protecting our educational and governmental institutions.

The Imperative for Regular Cybersecurity Assessments

National data underscores the effectiveness of regular cybersecurity maturity evaluations. Organizations that conduct consistent assessments demonstrate significantly higher maturity levels than those that do not. Both the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Cybersecurity and Infrastructure Security Agency (CISA) have highlighted the importance of these evaluations in their reports.

In its *K-12 Report: CIS MS-ISAC Cybersecurity Assessment of the 2022–2023 School Year*, MS-ISAC identifies K-12 schools as prime targets for cyber threat actors and recommends regular cybersecurity assessments.[1] Similarly, CISA's *Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats* advises schools to invest in impactful security measures and build toward a mature cybersecurity plan—reinforcing the necessity of regular assessments to inform these efforts.[2] Specifically, conducting assessments biennially allows organizations to devote alternate years to remediation, thereby strengthening their security posture. As experts note, "Regular cybersecurity assessments offer a critical opportunity to identify vulnerabilities before they can be exploited by malicious actors."[3]

[1] https://learn.cisecurity.org/2023-k12-report

[2] https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf

[3] https://cybsoftware.com/6-step-approach-to-how-organizations-can-carry-out-effective-cybersecurity-assessments/

Adherence to State Minimum Cybersecurity Standards

Aligning with established cybersecurity frameworks is a proven strategy to mitigate risks. Maryland's Minimum Cybersecurity Standards align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ensuring that organizations implement controls that bolster overall cybersecurity maturity while addressing specific vulnerabilities.[4] Several states have enacted legislation mandating compliance with these standards, reflecting a national trend toward strengthening cybersecurity across diverse sectors.[5]

Impact of Cybersecurity Breaches in Educational Institutions

The repercussions of cybersecurity incidents, such as ransomware attacks, in educational and government settings are severe. In Maryland, multiple school systems have experienced significant disruptions, leading to substantial financial burdens[6] and the exposure of confidential student data.[7] These incidents underscore the necessity of regular assessments to identify and address vulnerabilities proactively, reducing risks and preserving educational continuity.[8]

Support Mechanisms for Local School Systems

Recognizing that many school systems operate with limited resources—often relying on IT personnel who juggle multiple roles—the State has implemented supportive measures. During my tenure as Director of Local Cybersecurity, we collaborated with the Maryland Association of Boards of Education (MABE) to develop an assessment capability aligned to the SMCS, offered at no cost to members of MABE's insurance pool, covering 19 out of 24 jurisdictions. The State's Local Information Security Officer (ISO) program also provides a range of assessment services, bolstered by State and Local Cybersecurity Grant Program (SLCGP) funds.

Under Senate Bill 907, dedicating ISOs to public school systems would ensure they receive specialized assistance, staffing support, and the time needed to enhance their cybersecurity defenses in the most cost-effective manner possible. Shared service models such as these have proven to be among the most valuable whole-of-state strategies nationwide.

The Role of OLA Audits in Strengthening Cybersecurity

Office of Legislative Audits (OLA) reviews are a critical element in enforcing strong governance and compliance. OLA has done commendable work in identifying areas that need improvement.

[4] https://doit.maryland.gov/cybersecurity/Documents/CSF-Guidebook.pdf

[5] https://www.ncsl.org/technology-and-communication/cybersecurity-2023-legislation

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

[7] https://www.scworld.com/brief/almost-100k-impacted-by-maryland-school-district-ransomware-attack

[8] https://www.cisecurity.org/insights/white-papers/strengthening-critical-infrastructure-sltt-progress-priorities

However, because audits are time-consuming, this provision aims to reduce duplicative efforts and create a more efficient process. If OLA aligns its school system audits with the same state compliance requirements, it would greatly streamline documentation and discovery—using the very information schools already collect to meet Maryland's minimum cybersecurity standards. This approach will not only simplify the audit process but also ensure a consistent, structured framework for cybersecurity governance across the state's educational institutions.

Senate Bill 907 represents a pivotal step toward strengthening Maryland's educational cybersecurity infrastructure. In a time when budget constraints are significant and cybersecurity risks are at an all-time high and ever-evolving, it is incumbent upon us to embrace sensible, cost-effective strategies that bolster our State's resilience. By mandating compliance with State minimum cybersecurity standards and requiring regular maturity assessments, this bill ensures that vulnerabilities are systematically identified and addressed. The provision of dedicated support through the ISO program further empowers school systems to implement robust cybersecurity measures. Additionally, aligning OLA audits with State cybersecurity requirements will streamline the compliance process and reinforce a uniform standard of governance.

I respectfully urge the committee to issue a favorable report on SB907, reaffirming our shared commitment to protecting the integrity of Maryland's educational environment. Thank you for considering my testimony.

Sincerely,
Netta Squires, JD, MSL, CEM, CCRP
President, Cybersecurity Strategy and Resilience
Open District Solutions