Yelin Testimony - SB907 2025.pdf

Uploaded by: Ben Yelin

Position: FAV

SB0907 - CYBERSECURITY - STANDARDS, COMPLIANCE, AND AUDITS - ALTERATIONS

EDUCATION, ENERGY AND THE ENVIRONMENT

FAVORABLE

MARCH 5, 2025

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

My name is Ben Yelin, and I am the Program Director for Public Policy & External Affairs at the University of Maryland Center for Health and Homeland Security. I also served as the co-chair, with Senator Hester, of the Ad Hoc Subcommittee of the Maryland Cybersecurity Council on State and Local Cybersecurity. We recommended in our 2021 study that every unit of local government in Maryland conduct regular cybersecurity assessments. The General Assembly required these assessments in the 2022 cybersecurity reform legislative package.

The cyber threat to the K-12 education system is particularly acute. School districts face two particularly unique vulnerabilities. First, schools house sensitive data, such as Social Security numbers, addresses and other personally identifiable information (PII) of students, faculty and staff. Second, public school systems have been historically under-resourced. Particularly in smaller jurisdictions, school systems do not have the personnel, expertise or funds to protect their networks. As a result of these factors, attacks against K-12 schools have increased by nearly 400% over the past decade.

It is not just the frequency of attacks, but the severity of the impacts that are particularly problematic. According to a 2022 Government Accountability Office (GAO) report, the loss of learning due to cyber-attacks can range from 3 days to 3 months.[1] Costs of either paying ransoms or recovering networks range from $50,000 to up to $1 million. We have seen these impacts firsthand in Maryland. In the past several years, we have seen ransomware hacks against several Maryland school districts, most recently Prince George's County in 2023-2024. The most significant incident in Maryland affected the Baltimore County Public School system in 2020-2021. The incident caused vast interruptions to school operations, which were particularly damaging as most students were still in remote learning as part of the ongoing COVID-19 pandemic. An Inspector's General report in January 2023 estimated that the cost of the attack was as high as $10 million.[2]

SB907 is an important first step in protecting our schools from cyber-attacks. This bill builds on the 2022 cybersecurity package by requiring the Office of Security Management (OSM) to set minimum cybersecurity standards for local school systems. OSM is well situated to develop standards commensurate with best practices, and the bill allows flexibility by not being overly prescriptive as to which measures school systems should adopt. The bill would also assign at least three information

[1] https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done
[2] https://abcnews.go.com/US/baltimore-schools-failed-fully-act-security-recommendations-cyber/story?id=96671802#:~:text=The%20cyber%20attack%20cost%20the,%2410%20million%2C%20a%20report%20says.

security officers to support local school systems in complying with minimum cybersecurity requirements, conducting maturity assessments every two years, and with remediation efforts.

While there may be costs to the State and Counties associated with this bill, the costs pale in comparison to the devastating economic damage we could see in the coming years, as cyber criminals and foreign actors become more sophisticated.

For these reasons. I respectfully request a favorable report on SB907.

cth_written_testimony.pdf

Uploaded by: Charles Harry

Position: FAV

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

CA-2025-SB907-TESTIMONY-FAV.docx.pdf

Uploaded by: John Fiastro

Position: FAV

Cybersecurity Association

10440 Little Patuxent Pkwy
Floor 12
Columbia, MD 21044
+443-853-1970 ☎
info@cyber-association.com ✉
www.cyber-association.com

SB907 – Cybersecurity – Standards, Compliance, and Audits – Alterations
Senate Education, Energy, and the Environment Committee
March 5, 2025
Favorable

Dear Chair Feldman and Members of the Senate Education, Energy, and the Environment Committee,

My name is Tasha Cornish, and I am writing on behalf of the Cybersecurity Association, Inc. (CA), a nonprofit 501(c)(6) organization dedicated to strengthening Maryland's cybersecurity industry. Our association represents over 600 businesses ranging from small enterprises to large corporations employing nearly 100,000 Marylanders. We appreciate the opportunity to offer testimony in **favorable support** of Senate Bill 907, which aims to enhance cybersecurity standards across Maryland's local school systems.

Support for Enhanced Cybersecurity Requirements

The Cybersecurity Association strongly supports the provisions in SB907 that require local school systems to comply with the State Minimum Cybersecurity Standards established by the Department of Information Technology (DoIT). The inclusion of regular cybersecurity maturity assessments, dedicated cybersecurity personnel, and oversight mechanisms will significantly improve the cybersecurity resilience of Maryland's education system.

With schools becoming increasingly reliant on digital infrastructure, it is imperative to proactively address cybersecurity risks to protect students, educators, and sensitive data from cyber threats. Establishing these minimum standards ensures a consistent and enforceable approach to cybersecurity preparedness statewide.

Ensuring Feasible Implementation

While we support these necessary cybersecurity improvements, we recognize that implementation may require additional resources for some county boards of education. Many local school systems have varying levels of cybersecurity readiness, and achieving compliance with the new standards will require investments in personnel, assessments, and security controls. To ensure that all school systems can meet these important requirements, we encourage targeted funding support for those that may need assistance.

We urge the General Assembly to explore funding mechanisms to assist county boards that have not yet met the DoIT cybersecurity standards. Providing state-level grants, technical assistance, or financial incentives will help ensure equitable implementation across all school systems, particularly those with limited resources.

Recommendations for Implementation Support

To effectively implement SB907 while mitigating financial concerns, we recommend the following:

1. **Dedicated Funding for School Cybersecurity** – Establish a state funding mechanism to support county boards in meeting cybersecurity mandates.
2. **Expanded State-Level Assistance** – Increase the number of Information Security Officers assigned by DoIT to local school systems, providing hands-on guidance and technical support.
3. **Grant Opportunities and Federal Support** – Encourage collaboration with federal cybersecurity initiatives to secure additional funding and resources for Maryland schools.
4. **Flexible Compliance Timelines** – Allow phased implementation for county boards that require additional time and funding to reach compliance.

Conclusion

SB907 is a critical step toward strengthening cybersecurity protections in Maryland's education sector. The Cybersecurity Association fully supports the bill's objectives and urges the General Assembly to consider targeted funding solutions to facilitate implementation without placing undue financial strain on county boards.

We appreciate your commitment to advancing cybersecurity resilience across Maryland. Thank you for your time and consideration. I am happy to answer any questions the committee may have.

Hester SB 907 Testimony.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

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

THE SENATE OF MARYLAND
Annapolis, Maryland 21401

Testimony in Support of SB907 - Cybersecurity - Standards, Compliance, and Audits - Alterations

March 5, 2025

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

Thank you for your consideration of **SB907**, which strengthens cybersecurity protections for Maryland's public schools, ensuring they have the tools and resources necessary to prevent cyberattacks and comply with state security standards.

Cyberattacks on schools are **not just an IT issue**—they pose a **direct threat** to students, educators, and the integrity of our education system. Schools store vast amounts of sensitive personal data, including Social Security numbers, medical records, and financial information, making them prime targets for cybercriminals. A single cyberattack can **disrupt learning for weeks, expose students and staff to identity theft, and cost millions in recovery efforts**. Research shows that **U.S. schools lose an average of $550,000 per day of downtime** due to ransomware attacks, with **total recovery costs reaching millions of dollars**.[1]

The risks are real and growing. In August 2023, Prince George's County Public Schools fell victim to a cyberattack that compromised approximately 4,500 district user accounts, primarily those of staff members.[2] In 2020, a ransomware attack on Baltimore County Public Schools shut down virtual learning and required $9.7 million in recovery efforts.[3] Alarmingly, only 14% of schools currently require cybersecurity awareness training, leaving them highly vulnerable to phishing and other cyber attacks.[4]

[1] https://www.comparitech.com/blog/information-security/school-ransomware-attacks/

[2] https://www.wusa9.com/article/news/education/prince-georges-county-public-schools-cyberattack/65-55fb0ef7-1a50-4e8c-aa3d-995ef39cfef0

[3] https://www.wmar2news.com/news/local-news-in-maryland/investigative-report-reveals-what-led-to-2020-cyberattack-on-baltimore-county-public-schools

[4] https://www.route-fifty.com/cybersecurity/2025/01/parents-think-schools-cybersecurity-stronger-reality-report-says/401916/?oref=rf-today-nl&utm_source=Sailthru&utm_medium=email&utm_campaign=Route%20Fifty%20Today:%20January%208%2C%202025&utm_term=newsletter_rf_today

To bolster school cybersecurity and prevent future attacks, SB 907 establishes key standards for local education agencies (LEAs). Specifically, the bill:

1) **Strengthens Cybersecurity Staffing & Investments**
   - **a)** Requires LEAs to report IT staff expenditures, broken down by full-time employees, vendor-supported staff, and dedicated cybersecurity professionals.
   - **b)** Mandates that each county board provide sufficient cybersecurity staffing, as determined by the State Chief Information Officer.
   - **c)** Directs DoIT to assign at least three Information Security Officers to assist LEAs
   - **d)** Recognizes cybersecurity expenses as an allowable per-pupil cost under education technology funding in the Blueprint for Maryland's Future.
   - **e)** Allows school systems to share cybersecurity services, contractors, and regional support to maximize resources.
   - **f)** Establishes annual tracking and reporting of cybersecurity expenditures, starting August 15, 2025.
2) **Ensures Compliance with State Cybersecurity Standards**
   - **a)** Requires all LEAs to comply with and certify to state minimum cybersecurity standards by 2026.
   - **b)** Directs the Office of Security Management within DoIT to annually review and update state minimum cybersecurity standards to keep pace with evolving threats.
   - **c)** Mandates that all LEAs conduct cybersecurity maturity assessments every two years to evaluate preparedness and resilience.

This legislation was **developed in collaboration with chief information officers** from school systems across Maryland, who have emphasized the **urgent need for stronger cybersecurity protections**. By setting clear standards, increasing compliance, and prioritizing investment in cybersecurity, **SB 907 will help safeguard Maryland's schools, protect sensitive data, and prevent costly cyberattacks before they happen**.

For these reasons, I respectfully request a favorable report on SB 907.

Sincerely,

Katie Fry Hester

Senator Katie Fry Hester
Howard and Montgomery Counties

Squires Testimony in Support of Senate Bill 907.pd

Uploaded by: Netta Squires

Position: FAV

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

MD K12 TLF TLFCC SB0907 Support.pdf

Uploaded by: Richard Lippert

Position: FAV

Maryland K12 Technology Leadership Forum Board

TO: The Honorable Senator Brian Feldman
Education, Energy and the Environment Committee

FROM: Maryland K12 Technology Leadership Forum

RE: Senate Bill 907 – Cybersecurity, Standards, Compliance, and Audits – Alterations

DATE: March 3, 2025

POSITION: Support

The Maryland K12 Technology Leadership Forum strongly supports Senate Bill 907, introduced by Senator Hester, which seeks to enhance cybersecurity standards, compliance, and audits within Maryland's local school systems. As cyber threats continue to evolve, it is crucial to strengthen our state's cybersecurity infrastructure, ensuring the protection of sensitive data and safeguarding students, teachers, and staff from cyberattacks.

Cybercriminals are increasingly targeting school systems nationwide, employing ever-changing tactics to breach security defenses. Maryland has not been immune to these attacks. Local Educational Agencies (LEAs) have suffered two major ransomware incidents, multiple third-party vendor breaches affecting staff and student data, and other cyber incidents that required extensive mitigation efforts. These attacks have cost Maryland over 10 million dollars in recovery expenses, disrupted instructional time, and eroded public confidence in our school systems. Most concerning is the exposure of confidential staff and student data, which poses significant risks.

LEAs have made considerable progress in enhancing their cybersecurity capabilities through knowledge-building, partnerships, and proactive defense measures. However, many districts still lack sufficient staffing and resources to meet the increasing cybersecurity demands. Often, cybersecurity responsibilities are assigned to personnel who already have multiple duties, stretching their capacity to effectively safeguard school systems. Despite being proactive, districts must allocate limited funds across numerous competing priorities, making it challenging to maintain strong cybersecurity defenses.

Senate Bill 907 addresses these critical needs by requiring local school systems to:

- Comply with and certify adherence to the State's minimum cybersecurity standards.
- Conduct a cybersecurity maturity assessment every two years.
- Report on cybersecurity expenditures and staffing to ensure adequate protection.
- Receive assistance from dedicated information security officers to support compliance and remediation efforts.

- Align legislative audits with the Department of Information Technology’s State Minimum Cybersecurity Standards, reducing redundant audits and administrative burdens.

Technology audits are necessary tools for strengthening cybersecurity measures, but they are often time- and resource-intensive. This bill seeks to streamline the auditing process by ensuring all technology audits adhere to consistent standards. By establishing uniform criteria, school districts can avoid multiple redundant audits within the same fiscal year, reducing strain on limited resources.

Additionally, the bill would allow districts to use targeted per-pupil foundation funding for cybersecurity by expanding the list of associated costs to include cybersecurity measures and removing the prioritization of digital devices. This provision would provide schools with the flexibility needed to invest in robust cybersecurity staffing and defenses while maintaining other essential educational initiatives.

Accordingly, the MD K12 Technology Leadership Forum respectfully requests a **FAVORABLE** committee report on SB 907.

CA-2025-SB907-TESTIMONY-FAV.docx.pdf

Uploaded by: Tasha Cornish

Position: FAV

Cybersecurity
Association

10440 Little Patuxent Pkwy
Floor 12
Columbia, MD 21044
+443-853-1970 ☎
info@cyber-association.com ✉
www.cyber-association.com

SB907 – Cybersecurity – Standards, Compliance, and Audits – Alterations
Senate Education, Energy, and the Environment Committee
March 5, 2025
Favorable

Dear Chair Feldman and Members of the Senate Education, Energy, and the Environment Committee,

My name is Tasha Cornish, and I am writing on behalf of the Cybersecurity Association, Inc. (CA), a nonprofit 501(c)(6) organization dedicated to strengthening Maryland’s cybersecurity industry. Our association represents over 600 businesses ranging from small enterprises to large corporations employing nearly 100,000 Marylanders. We appreciate the opportunity to offer testimony in **favorable support** of Senate Bill 907, which aims to enhance cybersecurity standards across Maryland’s local school systems.

Support for Enhanced Cybersecurity Requirements

The Cybersecurity Association strongly supports the provisions in SB907 that require local school systems to comply with the State Minimum Cybersecurity Standards established by the Department of Information Technology (DoIT). The inclusion of regular cybersecurity maturity assessments, dedicated cybersecurity personnel, and oversight mechanisms will significantly improve the cybersecurity resilience of Maryland’s education system.

With schools becoming increasingly reliant on digital infrastructure, it is imperative to proactively address cybersecurity risks to protect students, educators, and sensitive data from cyber threats. Establishing these minimum standards ensures a consistent and enforceable approach to cybersecurity preparedness statewide.

Ensuring Feasible Implementation

While we support these necessary cybersecurity improvements, we recognize that implementation may require additional resources for some county boards of education. Many local school systems have varying levels of cybersecurity readiness, and achieving compliance with the new standards will require investments in personnel, assessments, and security controls. To ensure that all school systems can meet these important requirements, we encourage targeted funding support for those that may need assistance.

We urge the General Assembly to explore funding mechanisms to assist county boards that have not yet met the DoIT cybersecurity standards. Providing state-level grants, technical assistance, or financial incentives will help ensure equitable implementation across all school systems, particularly those with limited resources.

Recommendations for Implementation Support

To effectively implement SB907 while mitigating financial concerns, we recommend the following:

1. **Dedicated Funding for School Cybersecurity** – Establish a state funding mechanism to support county boards in meeting cybersecurity mandates.
2. **Expanded State-Level Assistance** – Increase the number of Information Security Officers assigned by DoIT to local school systems, providing hands-on guidance and technical support.
3. **Grant Opportunities and Federal Support** – Encourage collaboration with federal cybersecurity initiatives to secure additional funding and resources for Maryland schools.
4. **Flexible Compliance Timelines** – Allow phased implementation for county boards that require additional time and funding to reach compliance.

Conclusion

SB907 is a critical step toward strengthening cybersecurity protections in Maryland's education sector. The Cybersecurity Association fully supports the bill's objectives and urges the General Assembly to consider targeted funding solutions to facilitate implementation without placing undue financial strain on county boards.

We appreciate your commitment to advancing cybersecurity resilience across Maryland. Thank you for your time and consideration. I am happy to answer any questions the committee may have.