SB601 Testimony - EEE Committee 2.26.26.pdf
Uploaded by: Ben Yelin
Position: FAV

UNIVERSITY of MARYLAND BALTIMORE
CENTER FOR CYBER, HEALTH, AND HAZARD STRATEGIES

Testimony in Support of SB601: Cybersecurity - Standards and Compliance - Alterations.

Date: February 26, 2026

Committee: Education, Energy, and the Environment

Introduction

Chair Feldman, Vice Chair Kagan, and members of the Committee, thank you for the opportunity to provide testimony in support of SB601 – Cybersecurity - Standards and Compliance - Alterations. My name is Ben Yelin, and I serve as the Program Director for Public Policy & External Affairs at the University of Maryland Center for Cyber, Health and Hazard Strategies.

In 2021, I served as co-chair, alongside Senator Hester, of an ad hoc subcommittee within the Maryland Cybersecurity Council dedicated to State and Local Cybersecurity. Through our study, we recommended that every unit of local government in Maryland, including local school districts, conduct regular cybersecurity assessments. The General Assembly later codified this recommendation by requiring these assessments in the 2022 cybersecurity reform legislative package.

The Cyber Threat to K-12 Education

The cyber threat to the K-12 education system is especially severe. School districts face two distinct vulnerabilities. First, they store highly sensitive data, such as Social Security numbers, addresses, and other personally identifiable information (PII) related to students, faculty, and staff. Second, public school systems have historically lacked sufficient resources. This is particularly true in smaller jurisdictions, where school systems often do not possess the necessary personnel, expertise, or funding to adequately protect their networks. As a result of these combined factors, cyberattacks targeting K-12 schools have increased by nearly 400% over the past decade.

Impact of Attacks on Schools

It is not only the growing frequency of these attacks that poses concern, but also the severity of their consequences. A 2022 report from the Government Accountability Office (GAO) found that the loss of instructional time due to cyberattacks can range from three days to three months. The costs associated with either paying ransoms or recovering compromised networks can span from $50,000 to as much as $1 million. Maryland has experienced these impacts firsthand.

UNIVERSITY of MARYLAND BALTIMORE
CENTER FOR CYBER, HEALTH, AND HAZARD STRATEGIES

In recent years, several Maryland school districts have fallen victim to ransomware attacks, most notably Prince George's County during the 2023-2024 school year. The most significant incident occurred in the Baltimore County Public School system during 2020-2021. This event caused major disruptions to school operations, which were particularly damaging as most students were still engaged in remote learning due to the ongoing COVID-19 pandemic. According to a January 2023 Inspector General's report, the cost of this attack was estimated as high as $10 million.

Provisions of SB601

SB0601 is a pragmatic measure designed to strengthen the cyber readiness of our public schools and ensure they are prepared to address emerging cyber threats. The bill introduces several key provisions:

- Each school system must designate a point-of-contact for all cybersecurity-related matters. This will enable the State Chief Information Security Officer (SCISO) to have a liaison in every jurisdiction, facilitating the timely exchange of critical information about new cyber threat vectors.
- All school systems will be required to comply with State minimum cybersecurity standards established by the Department of Information Technology (DoIT) and to conduct cybersecurity maturity assessments every two years.
- The bill broadens the allowable uses of funding under the Blueprint for Maryland's Future to authorize expenditures on cybersecurity. Investing in the protection of our systems and networks is as essential as any other IT expenditure, as it helps prevent extended disruptions or significant costs associated with ransom payments or restoring connectivity.
- The Office of Security Management will be required to review and update the minimum cybersecurity standards annually. Since the cybersecurity threat landscape evolves rapidly, frequent reviews and updates to these standards will benefit units of government, including school districts.

Conclusion

SB601 constitutes a critical and worthwhile investment in the cyber readiness of Maryland's public schools. By strengthening our defenses, we can ensure continuous, uninterrupted education for all Maryland public school students. For these reasons, I respectfully request a favorable report on SB601.

SB 601 - Cybersecurity - Standards and Compliance.
Uploaded by: Denise Riley
Position: FAV

A Union of Professionals
AFT-Maryland

5800 Metro Drive, Suite 100 • Baltimore, MD 21215-3226
410/764-3030 • fax: 410/764-3008
md.aft.org

Kenya Campbell
PRESIDENT

LaBrina Hopkins
SECRETARY-TREASURER

Written Testimony to the Senate Education, Energy, and the Environment Committee
SB 601 - Cybersecurity - Standards and Compliance - Alterations
February 26, 2026

FAVORABLE

Chair Feldman, Vice Chair Kagan and Members of the Committee: AFT Maryland urges a favorable report on Senate Bill 601. As our state's infrastructure and government services become increasingly digital, the threat of cyber-attacks has never been higher. SB 601 provides a necessary update to Maryland's cybersecurity framework by refining our standards and ensuring that both state agencies and their partners are held to a consistent, high level of security.

The bill focuses on aligning Maryland's requirements with updated best practices. Technology moves fast, and static laws quickly become obsolete. SB 601 helps to ensure that our minimum standards are effective against modern threats. This isn't just about checking a box; it's about creating a culture of accountability. By clarifying which entities must comply and how that compliance is verified, the bill closes dangerous gaps that hackers often exploit to gain access to state networks through third-party vendors or local government systems.

The alterations proposed in SB 601 help streamline the reporting and oversight process. In the event of a security incident, time is the most valuable resource. This bill helps ensure that communication between agencies and the Office of Security Management is clear and efficient, to allow a faster coordinated response to mitigate damage. It also provides a more realistic and enforceable framework for local governments, acknowledging that while security is mandatory, the path to achieving it must be clear and supported by state-level guidance.

SB 601 is a common-sense measure to protect Maryland's digital borders and the private data of our residents. It ensures that our state remains a leader in cybersecurity and that our public institutions are resilient against the evolving landscape of digital crime. For these reasons we urge a favorable report. Thank you.

SB0601.pdf
Uploaded by: James Corns
Position: FAV

Having navigated a massive cyberattack and its recovery, I can attest to the impact these events have on school systems. SB0601(HB0957) seeks to spotlight standards and practices to mitigate cybersecurity risks.

Local Educational Agencies (LEAs) within the State of Maryland sit in a unique spot between a local and state agency. When laws are enacted, the term state agency is often used to define its scope. In the past, this has sometimes left in question whether or not LEAs were included. In my opinion, SB0601 clearly defines requirements for cybersecurity specific to LEAs. Given the potential instructional impact, scope of stored data, and impact on public confidence, required minimum specifications must be in place to maximize the security protecting these LEA aspects.

While much of these requirements are implied or hinted at in other legislation, SB0601 focuses a spotlight on the requirements of LEAs to protect their technology ecosystems, leaving no question that cybersecurity has moved past best practices and to essential to operations of the LEA.

This bill will put in place requirements for the essential security practices that would have most likely prevented the attack I experienced and the year of hard-fought recovery I led. Technology is no longer a nice to have feature in education. It permeates every aspect of the school day. This bill acknowledges this and puts in place reasonable expectations for LEAs to meet. For these reasons, I support SB0601(HB0957) as written.

Jim Corns

Final_ Hester SB 601 Testimony (1).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

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

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

Testimony in Support of SB601 - Cybersecurity - Standards and Compliance - Alterations

February 24, 2026

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

Thank you for your consideration of SB601, 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] In 2025, Baltimore City Public Schools were again targeted, this time by the group Cloak, which stole more than 25,000 users' personal information and posted a portion of it on the dark web.[4] Alarmingly, only 14% of

[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.wbaltv.com/article/cyberattack-baltimore-city-public-schools-students-staff-cloak/64543595

schools currently require cybersecurity awareness training, leaving them highly vulnerable to phishing and other cyberattacks.[5]

This legislation is the product of many years of conversations and collaboration with chief information officers from school systems across Maryland, who have emphasized the urgent need for stronger cybersecurity protections. Through years of working with them, we have identified the major barriers to strengthening school cybersecurity: a lack of boots on the ground and limited enforcement capability. This bill provides them with state standards and resources to overcome these identified barriers.

To bolster school cybersecurity and prevent future attacks, SB601 establishes key standards for local education agencies (LEAs). Specifically, the bill:

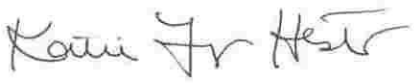
1) **Strengthens Cybersecurity Staffing and Investments**
    - **a)** Requires County Boards to identify a Local Point of Contact for all Cybersecurity-related communications and report this to the State Chief Information Security Officer.
    - **b)** Includes cybersecurity expenditures related to meeting the minimum standards as an allowable per-pupil Blueprint technology cost.
    - **c)** Requires DoIT's Information Security Officers to support local school systems in complying with standards, conducting maturity assessments, and undertaking remediation efforts.
2) **Ensures Compliance with State Cybersecurity Standards**
    - **a)** Mandates that each local school system certify compliance with State Minimum Cybersecurity Standards to the Office of Security Management within the Department of Information beginning in 2027 and every two years thereafter.
    - **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.

By setting clear standards, increasing compliance, and prioritizing investment in cybersecurity, SB601 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 SB601.

Sincerely,

---

[5] 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



Senator Katie Fry Hester
Howard and Montgomery Counties

Senator Hester SB601 Support Letter.pdf
Uploaded by: Mike Centrella
Position: FAV

SecurityScorecard

The Honorable Katie Fry Hester
Miller Senate Office Building
Annapolis, MD 21401

Senate Bill 601 – Cybersecurity – Standards and Compliance – Alterations: Support

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

I respectfully submit this letter in support of SB 601, Cybersecurity – Standards and Compliance – Alterations.

As a former senior executive with the United States Secret Service with more than 25 years of experience addressing complex national security and cyber-enabled threats, and now serving as Head of Public Policy at SecurityScorecard, where I work with federal, state, and local governments to strengthen cyber risk management practices, I have seen firsthand how K–12 institutions have become frequent targets of ransomware, data theft, and third-party compromise. Schools are not only educational institutions, they are critical infrastructure within our communities.

SB 601 takes an important and responsible step by requiring local school systems to comply with State Minimum Cybersecurity Standards, conduct recurring cybersecurity maturity assessments, and formally certify compliance. These provisions introduce measurable accountability and continuous improvement; core principles of modern cybersecurity governance aligned with nationally recognized NIST best practices.

This legislation is particularly important because it shifts cybersecurity from voluntary guidance to structured, verifiable standards. Clear requirements for designated local points of contact, standardized reporting, and recurring assessments will significantly improve coordination, transparency, and incident response effectiveness across the State.

Recognizing cybersecurity as an authorized education technology expenditure is also a critical and practical update. School systems must have the flexibility to invest in protective controls, risk visibility tools, and remediation efforts that safeguard student data and ensure operational continuity. As implementation progresses, scalable and data-driven approaches, particularly those that provide objective risk measurement and continuous monitoring, will help school systems meet compliance obligations efficiently and cost-effectively.

SecurityScorecard, Inc.
1140 Avenue of Americas, 19th Floor
New York, NY 10036

Michael.Centrella@securityscorecard.io
info@securityscorecard.com
Main (800) 682-1707

Maryland has an opportunity to lead by pairing clear statutory standards with modern risk management practices that strengthen resilience across all local school systems. SB 601 establishes a strong policy framework that supports that goal.

For these reasons, I respectfully urge a favorable report on SB 601. I appreciate your leadership on this important issue and would welcome the opportunity to serve as a resource as the bill advances or as implementation planning begins.

Respectfully submitted,

Michael R. Centrella

Head of Public Policy, SecurityScorecard

For any questions or more information regarding SSC's position, please contact Michael.Walsh@capitol-strategies.com

Squires Testimony SB601.pdf
Uploaded by: Netta Squires
Position: FAV

Testimony in Support of Senate Bill 601: Cybersecurity – Standards and Compliance – Alterations

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 601, which seeks to enhance the cybersecurity posture of Maryland's local school systems by mandating adherence to State Minimum Cybersecurity Standards (SMCS), requiring biennial cybersecurity maturity assessments, and establishing local points of contact for cybersecurity communications. Over the past two decades, I have served in public safety and cybersecurity roles—including having the honor and pleasure of 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 the Center for Critical Infrastructure Security (CCIS), a Maryland nonprofit focused on cybersecurity and operational resilience for organizations serving basic community needs, as well as being the Founder and President of Open District Solutions, as organization supporting resilience state, local, and education communities. 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. 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. Specifically, conducting assessments biennially allows organizations to devote alternate years to remediation, thereby strengthening their security posture.

Designating Local Points of Contact

Senate Bill 601 wisely requires each local school system to designate a local point of contact for cybersecurity communications. This provision addresses a persistent challenge: when cybersecurity incidents or vulnerabilities arise, there is often no clearly identified individual at the local level to receive and act on critical information from State agencies. A designated point of contact ensures that threat intelligence, compliance guidance, and incident response coordination flow efficiently

between the State and local school systems. This simple but essential step will materially improve the speed and effectiveness of cybersecurity communications statewide.

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. Several states have enacted legislation mandating compliance with these standards, reflecting a national trend toward strengthening cybersecurity across diverse sectors. SB 601's requirement that school systems not only comply with but also certify compliance with these standards adds an important layer of accountability and governance.

Annual Updates to State Minimum Cybersecurity Standards

The bill's requirement that the Office of Security Management within the Department of Information Technology annually update the SMCS reflects the reality that the threat landscape evolves continuously. Standards that remain static quickly become inadequate. Annual updates ensure that Maryland's cybersecurity requirements keep pace with emerging threats, new technologies, and evolving best practices—providing school systems with current, actionable guidance rather than outdated benchmarks.

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 and the exposure of confidential student data. These incidents underscore the necessity of regular assessments to identify and address vulnerabilities proactively, reducing risks and preserving educational continuity.

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 601, 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. 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 601 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, requiring regular maturity assessments, establishing designated points of contact, and ensuring the standards themselves are annually updated, this bill provides a comprehensive, practical framework for protecting Maryland's school systems. 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 SB 601, 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 of Cybersecurity and Resilience
Open District Solutions
And
Executive Director
Center for Critical Infrastructure Security (CCIS)

Senate Bill 601 - DoIT Written Testimony.docx.pdf
Uploaded by: Sara Elalamy
Position: FWA

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

TO: Senate Education, Energy, and the Environment Committee
FROM: Department of Information Technology
RE: Senate Bill 601 - Cybersecurity - Standards and Compliance - Alterations
DATE: February 26, 2026
POSITION: Support with Amendments

The Honorable Brian J. Feldman, Chair
Senate Education, Energy, and the Environment Committee
2 West, Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chairman Feldman,

The Department of Information Technology (DoIT) respectfully submits this letter in support of Senate Bill 601, with amendments.

SB 601 reflects an important commitment to strengthening cybersecurity capacity within Maryland's local school systems. DoIT shares the goal of improving coordination and ensuring schools have access to cybersecurity expertise and resources as threats continue to evolve.

However, as drafted, the bill may unintentionally create ambiguity regarding DoIT's role and could impose operational responsibilities that extend beyond the Department's enterprise governance function. DoIT's role is to provide leadership, guidance, and subject matter expertise, not to assume day-to-day operational management of local systems.

To better align the bill with this intent while preserving meaningful support for local school systems, DoIT respectfully supports the following amendments:

Amendment No. 1

On page 1, in line 9, after "and" insert ", if necessary,"; in line 10, strike "support" and substitute "advise"; in the same line, strike "with" and substitute "on"; and strike beginning with "and" in line 10 down through "year" in line 11.

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

Amendment No. 2

On page 2, in line 9, strike “COUNTY BOARD” and substitute “LOCAL SCHOOL SYSTEM”.

On page 3, in line 8, strike the second “and”; in line 9, strike the comma and substitute “AND”; in line 10, strike the first comma; in the same line, strike “information technology staff, AND CYBERSECURITY” and substitute “; AND (9) CYBERSECURITY SERVICES, TECHNOLOGY, AND STAFF”; and in line 19, strike “county board” and substitute “LOCAL SCHOOL SYSTEM”.

On page 6, in line 9, after “AND” insert “, IF NECESSARY,”; in line 28, after “(D)” insert “(1)”; in the same line, strike “THE DEPARTMENT’S INFORMATION SECURITY OFFICERS” and substitute “ON REQUEST, THE DEPARTMENT”; in line 29, strike “SUPPORT” and substitute “ADVISE”; in the same line, strike “WITH” and substitute “ON”; and in lines 30 and 32, strike “(1)” and “(2)”, respectively, and substitute “(I)” and “(II)”, respectively.

On page 7, in line 2, strike “(3)” and substitute “(III)”; after line 2, insert:

“(2) THE DEPARTMENT IS NOT RESPONSIBLE FOR THE SUCCESSFUL PERFORMANCE OF OR DAY–TO–DAY MANAGEMENT OF THE DUTIES OF A LOCAL SCHOOL SYSTEM DESCRIBED IN PARAGRAPH (1) OF THIS SUBSECTION.”; and strike beginning with the second comma in line 16 down through “That” in line 19.

These amendments clarify that DoIT’s role is to provide advisory support when requested, while preserving the operational responsibility of local school systems for their own cybersecurity programs. This ensures the bill strengthens coordination without creating unintended mandates or shifting accountability.

With these amendments, DoIT believes SB 601 can effectively support cybersecurity resilience across Maryland’s education sector in a manner consistent with existing governance frameworks.

Best,

Katie Savage
Secretary
Department of Information Technology