

**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 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.<sup>1</sup>

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.<sup>2</sup> In 2020, a ransomware attack on Baltimore County Public Schools shut down virtual learning and required \$9.7 million in recovery efforts.<sup>3</sup> 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.<sup>4</sup> Alarming, only 14% of

---

<sup>1</sup> <https://www.comparitech.com/blog/information-security/school-ransomware-attacks/>

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

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

<sup>4</sup> <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.<sup>5</sup>

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,

---

<sup>5</sup>

[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](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)

Katie Fry Hester

Senator Katie Fry Hester  
Howard and Montgomery Counties