MABE
MARYLAND ASSOCIATION OF BOARDS OF EDUCATION

621 Ridgely Avenue, Suite 300, Annapolis, Maryland 21401
410-841-5414 · 800-841-8197 · Fax: 410-841-6580 · MABE.org

BILL:	**Senate Bill 601**
TITLE:	**Cybersecurity – Standards and Compliance - Alterations**
HEARING DATE:	**April 2, 2026**
POSITION:	**Letter of Information**
COMMITTEE:	**House Government, Labor, and Elections Committee**
CONTACT:	**Sam Mathias, Legal & Policy Director (smathias@mabe.org)**

The Maryland Association of Boards of Education (MABE), representing all the State's local boards of education, provides this informational letter for Senate Bill 601, **Cybersecurity – Standards and Compliance – Alterations.**

Senate Bill 601 would codify elements of current school system practice into law. Specifically, the bill enables the State Department of Information Technology (DoIT) to establish State Minimum Cybersecurity Standards, requires school systems to conduct a cybersecurity maturity assessment every 2 years either with DoIT or a state-approved vendor, and requires that each local school system certify that it complies with state minimum cybersecurity standards.

While all school systems are committed to maintaining strong cybersecurity, the bill's certification requirement, absent any of the flexibility currently afforded school systems, does not account for the significant and ongoing costs associated with meeting evolving minimum standards. Cybersecurity is not a one-time investment; it requires continuous expenditures on enterprise security tools, network protections, threat monitoring, data security, email security, staff training, and regular independent assessments. For a system the size of Prince George's County Public Schools, for example, these costs are estimated to exceed $2 million annually, and similar pressures exist across other local systems.

Given that the State, through DoIT, will define and update the applicable standards over time, local school systems will be required to meet requirements without clear predictability as to scope or cost. Cybersecurity should not be solely a local obligation; it is a matter of statewide interest and statewide risk. Requiring certification without corresponding flexibility in standards, or financial support, effectively shifts substantial and ongoing responsibility to local school systems, which must already make difficult choices within constrained budgets. At a minimum, the certification framework should retain the flexibility reflected in current practice between DoIT and local school systems, where school systems conduct self-assessments and, in areas where they do not meet current standards, develop plans in partnership with DoIT to address and remediate identified gaps. Ideally, the State should provide dedicated, sustained funding to support

compliance, ensuring that school systems can meet cybersecurity standards responsibly without diverting resources from core educational needs.

MABE appreciates the General Assembly's commitment to strengthening cybersecurity across Maryland's public education system. We respectfully urge consideration of the cost, flexibility, and implementation concerns outlined above to ensure that this framework is both effective and sustainable for local school systems.