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.