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.