Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
Third Reader

House Bill 38 (Delegate Carey)
Health and Government Operations Education, Health, and Environmental Affairs

State Government – Department of Information Technology – Cybersecurity

This bill expands the responsibilities of the Secretary of Information Technology to include advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy and, in consultation with the Attorney General, (1) advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions of higher education, and (2) developing guidance on consistent cybersecurity strategies for counties, municipal corporations, school systems, and all other political subdivisions of the State. None of the Secretary's new responsibilities may be construed as establishing a mandate for any of these local government entities.

Fiscal Summary

State Effect: The Department of Information Technology (DoIT) can likely handle the bill's requirements using existing budgeted resources, as discussed below. The Attorney General's Office, Legislature, and Judiciary can continue to consult with DoIT using existing resources. Revenues are likely not affected, as discussed below.

Local Effect: No direct effect on local governmental finances; local governmental entities may elect to implement or not implement cybersecurity-related guidance provided by DoIT.

Small Business Effect: None.

Analysis

Bill Summary: "Cybersecurity" means processes or capabilities wherein systems, communications, and information are protected and defended against damage,

unauthorized use or modification, and exploitation. "Cybersecurity strategy" means a vision, a plan of action, or guiding principles.

Current Law: DoIT and the Secretary of Information Technology are responsible for:

- developing and enforcing information technology (IT) policies, procedures, and standards;
- providing technical assistance, advice, and recommendations to any unit of State government;
- reviewing agency project plans to make information and services available to the public over the Internet;
- developing and maintaining a statewide IT master plan, as specified; and
- adopting and enforcing nonvisual access standards to be used in the procurement of IT services, as specified.

The following agencies are exempt from oversight by DoIT:

- public institutions of education for academic or research purposes;
- the Maryland Port Administration (MPA);
- the University System of Maryland (USM);
- St. Mary's College of Maryland;
- Morgan State University; and
- the Maryland Stadium Authority.

Background: For more information on cybersecurity issues in the State and across the nation, please see the **Appendix – Cybersecurity.**

State Fiscal Effect: DoIT currently advises and oversees most State agencies with regards to their cybersecurity strategies and systems and has recently developed a State of Maryland Information Technology Security Manual to guide cybersecurity practices in the State, as discussed in the appendix. DoIT does not, however, directly provide any similar cybersecurity services for counties, municipal corporations, school districts, or other political subdivisions of the State at this time. Even so, DoIT can likely meet the bill's requirements at little to no cost by modifying its existing cybersecurity manual, if necessary, and providing it to these local government entities.

This analysis assumes that DoIT's oversight of the cybersecurity strategy for State agencies specifically exempt from other DoIT oversight (MPA, USM, *etc*.) is merely providing those agencies with the manual that has already been developed and being available for advice and consultation. Thus, DoIT is already meeting the bill's requirement that it

oversee a consistent cybersecurity strategy for State agencies, including advising and consulting with the Legislative and Judicial branches. However, to the extent that the bill is interpreted to require DoIT to more closely oversee the cybersecurity strategies of agencies that are currently exempt from its oversight, reimbursable revenues and expenditures for DoIT increase commensurately as it provides services for those agencies as well (and expenditures for those agencies also increase).

Additional Information

Prior Introductions: HB 235 of 2020, as amended, passed the House and was referred to the Senate Education, Health, and Environmental Affairs Committee, but no further action was taken. Its cross file, SB 120, received an unfavorable report from the Senate Education, Health, and Environmental Affairs Committee.

Designated Cross File: SB 49 (Senator Lee) - Education, Health, and Environmental Affairs.

Information Source(s): Department of Information Technology; Office of the Attorney General; Judiciary (Administrative Office of the Courts); Maryland Department of Transportation; University System of Maryland; Caroline, Howard, Montgomery, and Prince George's counties; Maryland Association of Counties; Maryland Municipal League; Baltimore City Public Schools; Baltimore County Public Schools; Anne Arundel County Public Schools; Frederick County Public Schools; St. Mary's County Public Schools; Department of Legislative Services

Fiscal Note History: First Reader - January 19, 2021
rh/mcr Third Reader - February 24, 2021

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510

Appendix – Cybersecurity

Cybersecurity Issues

In recent years, cybersecurity and privacy issues have received significant attention from the general public and policymakers as a result of the many ransomware attacks, data breaches, and other cyberattacks that have taken place in the nation and the State. Globally, in 2019 and 2020, the Center for Strategic and International Studies identified over 200 cyberattacks and data breaches (many of which involved the United States) involving (1) government agencies; (2) defense and high tech companies; or (3) economic crimes with losses of more than $1 million. For example, in November 2020, Baltimore County Public Schools' information technology (IT) systems were made unusable by a ransomware attack and the personally identifiable information (PII) of 27.7 million Texas drivers was exposed in a data breach.

In 2019, governments in the State experienced numerous cyberattacks and breaches. Most notably, Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks. Similarly, the Maryland Department of Labor's licensing database was breached, and PII of as many as 78,000 licensees may have been accessed by the hackers.

Recent State Action

In June 2019, the Governor signed Executive Order 01.01.2019.07, which creates the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative creates the Office for Security Management within the Department of Information Technology (DoIT) and charges the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch IT systems. The office is led by the State chief information security officer (SCISO), who is appointed by the Governor. The order also established the Maryland Cybersecurity Coordinating Council to assist SCISO and the office in their duties.

In that same month, DoIT released the State of Maryland Information Technology Security Manual. The manual currently serves as the primary policy for establishing and defining the State's IT security practices and requirements; all State agencies are required to adhere to the manual.

Legislation enacted in 2020 expands and enhances the cybersecurity protocols that govern the collection, processing, sharing, and disposal of PII by public institutions of higher education in the State beginning on October 1, 2024.

Audits of State Agency Cybersecurity Discover PII Vulnerabilities

Over the 2019 interim, the Office of Legislative Audits (OLA) summarized its recent audit findings related to cybersecurity and PII and reported those findings to the Joint Audit and Evaluation Committee in December 2019. OLA found that, from July 2013 through December 2019, approximately 37.9 million PII records existed in State and local government agencies that were not adequately protected with data security controls. Over that same period, 77 of OLA's audits contained findings related to PII. While DoIT and the State have been improving their protection of PII, a 2020 legislative audit found additional issues. For example, in one instance PII was not adequately restricted to employees who should have access to it and instead was visible to over 5,000 State employees.

OLA has previously emphasized the financial cost associated with data breaches by citing the Ponemon Institute, an independent research organization focused on data protection, and IBM, one of the largest computer manufacturers in the world. The two organizations annually publish a report on global data breaches and their economic impacts. The 2020 Cost of a Data Breach Report found:

- the average total cost of a data breach in the United States is $8.6 million; and
- customer PII has the highest cost per record at $150. *For illustrative purposes,* costs for Texas could total $4.2 billion, as a result of the 27.7 million breached records discussed above.

These costs include detection of the breach, escalation, notifications, response, and lost business.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures (NCSL) advises that 38 states, the District of Columbia, and Puerto Rico introduced or considered about 280 bills or resolutions that dealt significantly with cybersecurity in 2020. Some of the key cybersecurity issues considered included:

- requiring government agencies to implement training or specific types of security policies and practices and improving incidence response and preparedness;

- increasing penalties for computer crime or addressing specific crimes, *e.g.*, ransomware;
- regulating cybersecurity within the insurance industry or addressing cybersecurity insurance;
- creating task forces, councils, or commissions to study or advise on cybersecurity issues; and
- supporting programs or incentives for cybersecurity training and education.

Moreover, NCSL reports that 19 states (including Maryland) adopted or enacted significant cybersecurity-related legislation in 2020. Notably, (1) Delaware granted its Department of Technology and Information the authority to develop and implement a comprehensive security program; (2) Georgia is using funds from its Revenue Shortfall Reserve to enhance cybersecurity technologies; (3) Louisiana enacted 10 pieces of legislation to significantly enhance its cybersecurity framework; and (4) Virginia required its chief information officer to develop and annually update a training program for all state employees in security awareness and in procedures for detecting, assessing, reporting, and addressing information security threats.

Notably, in 2019, 31 states adopted or enacted significant cybersecurity-related legislation. Most notably, (1) New York City enacted the Stop Hacks and Improve Electronic Data Security Act, which amended the state's data breach notification law and imposed more expansive data security requirements on companies; (2) Alabama, Delaware, Mississippi, and New Hampshire enacted legislation establishing a comprehensive security framework that insurance companies must implement; and (3) Oregon enacted legislation requiring manufacturers of "connected devices" to equip those devices with reasonable security features.