SB 917

Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 917 (Senator Hester)(By Request - Joint Cybersecurity, Information Technology, and Biotechnology Committee)

Budget and Taxation

Department of Information Technology - Status of Information Technology and Cybersecurity in State and Local Agencies

This bill requires each State agency in the Executive Branch and each local agency (meaning a county, county board of health, or county board of education) to annually (1) complete a cybersecurity preparedness assessment and (2) report (by September 1) specified information technology (IT) and cybersecurity information, including the findings of the assessment, to the Department of Information Technology (DoIT). DoIT must then annually (by December 31) compile, analyze, and report the information to each State and local agency and the General Assembly.

Fiscal Summary

State Effect: General fund expenditures increase by $250,000 in FY 2022 for programming costs and by $429,000 in FY 2023 due to staffing changes; out-year expenditures reflect ongoing operating costs, elimination of one-time costs, and savings from no longer using contractors. Reimbursable expenditures by DoIT increase by approximately $10.0 million annually beginning in FY 2022 for cybersecurity preparedness assessments for State agencies; State expenditures (all funds) and reimbursable revenues increase correspondingly as DoIT is repaid by the agencies for the assessments.

($ in millions)	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026
ReimB. Rev.	$10.00	$10.00	$10.00	$10.00	$10.00
GF Expenditure	$0.25	$0.43	$0.42	$0.45	$0.48
GF/SF/FF Exp.	$10.00	$10.00	$10.00	$10.00	$10.00
ReimB. Exp.	$10.00	$10.00	$10.00	$10.00	$10.00
Net Effect	($10.25)	($10.43)	($10.42)	($10.45)	($10.48)

Note:() = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease

Local Effect: Local expenditures increase, potentially significantly, to obtain cybersecurity preparedness assessments and modify IT systems, if necessary, to ensure county agencies are capable of providing information to DoIT. Revenues are not affected. **This bill imposes a mandate on a unit of local government.**

Small Business Effect: Meaningful.

Analysis

Bill Summary: The information submitted to DoIT by units of State government and local agencies must include, for the previous fiscal year and current fiscal year, (1) the number of IT staff positions, including vacant positions; (2) the ratio of IT employees to noninformation technology employees; (3) the unit's or local agency's IT budget, broken down as specified; (4) any major IT initiatives the unit or local agency is taking to modernize its IT systems; (5) initiatives to test and improve cybersecurity and data protection; (6) IT initiatives to improve customer access to State and local services; and (7) plans for future fiscal years to implement IT goals.

The report provided to each State agency, local agency, and the General Assembly by DoIT must include the compiled and analyzed information provided by State and local agencies and include recommendations for best practices to achieve efficiency and security in providing IT services and potential cost saving strategies. The information in the report must be broken down by unit or local agency, fiscal year, budget category, and issues identified by the cybersecurity preparedness assessments.

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

- developing and enforcing 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 (ITMP), as specified; and
- adopting and enforcing nonvisual access standards to be used in the procurement of IT services, as specified.

Specifically related to the ITMP, each unit of State government is generally required to develop and submit to the Secretary of Information Technology the following: (1) IT policies and standards; (2) an IT plan; and (3) an annual project plan outlining the status of

efforts to make information and services available to the public over the Internet. The IT plan of each unit of State government must be consistent with the statewide ITMP.

In addition to the Legislative Branch and the Judiciary, the following agencies are generally exempt from oversight by DoIT:

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

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

State Expenditures:

Department of Information Technology – Reporting Costs and Savings

DoIT advises that it intends to implement the bill by modifying its existing process for collecting and analyzing ITMP information provided to it by State agencies each year. DoIT's current process requires agencies to submit the information through a database application designed specifically for that purpose, and DoIT utilizes two contractors at an annual cost of $500,000 to (1) assist State agencies in developing and submitting the information and (2) analyze the submissions and prepare any necessary reports.

The bill dramatically expands DoIT's responsibilities with respect to collecting, analyzing, and reporting IT and cybersecurity information. In addition to adding DoIT oversight of all county governments (including school boards and health departments), the bill requires DoIT to review and analyze cybersecurity assessments from all State and local agencies, and to report the resulting information with greater specificity and granularity. In implementing the bill, DoIT will (1) modify its ITMP database application to accept the new information from State and local agencies and (2) replace its two contractors with eight permanent full-time staff. Given the expansion of the responsibilities for DoIT, full-time permanent staff are more appropriate to handle the combined ITMP and IT/cybersecurity reporting responsibilities under the bill.

Due to the bill's September 1 submission deadline for the IT/cybersecurity information and October 1, 2021 effective date, fiscal 2023 is the first year that State and local agencies must provide information to DoIT. To ensure the system is functional in fiscal 2023, the

necessary programming costs are assumed to be borne by DoIT in fiscal 2022. However, staffing changes are delayed until the beginning of fiscal 2023 (July 1, 2022), which still allows the new staff to assist State and local agencies in providing the information as required by September 1, 2022. Accordingly, general fund expenditures for DoIT increase by $250,000 in fiscal 2022 only for programming costs and increase by $429,074 in fiscal 2023, when DoIT's contractors are replaced by eight full-time permanent program managers. This level of staffing is needed to collect and analyze the new information from State agencies and the new information from a significant number of local agencies. The estimate for fiscal 2023 includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	8.0
Salaries and Fringe Benefits	$883,114
Contractor Savings	-500,000
Operating Expenses	45,960
Total FY 2023 Expenditures	**$429,074**

Future year expenditures reflect salaries with annual increases and employee turnover, ongoing operating expenses, termination of one-time costs, and ongoing savings due to no longer using contractors.

Cybersecurity Preparedness Assessments – State Agencies

Some State agencies may be able to obtain the cybersecurity preparedness assessments required by the bill (in some years) at no charge from the federal Cybersecurity and Infrastructure Security Agency (CISA). CISA provides a variety of cybersecurity assessments to State and local governments and critical infrastructure owners and assists those entities in enhancing their cybersecurity framework and practices based on the results. Even so, CISA has previously advised that it receives a significant number of requests for services each year, and generally prioritizes critical infrastructure and safety entities. As such, it is unclear how many State or local agencies will be able to obtain these assessments in any future year.

Thus, most State agencies experience annual costs to obtain the cybersecurity preparedness assessments; the precise cost to each agency depends on the structure, complexity, and condition of the agency's IT infrastructure. On average, cybersecurity assessments of the kind required by the bill cost between $75,000 and $100,000 per IT system. DoIT advises that the State has approximately 125 different systems spanning all Executive Branch agencies, so the total cost of conducting annual assessments is approximately $10.0 million. Costs may vary to the extent that some State agencies obtain assessments at no cost from CISA (as noted above) or engage private cybersecurity firms to obtain the assessments; however, it is unclear at this time whether CISA has the capacity to conduct

annual assessments on a large scale. *For illustrative purposes*, a preliminary search by the Department of Legislative Services identified private business cybersecurity preparedness assessment costs ranging from tens of thousands of dollars to hundreds of thousands of dollars per assessment, depending on the factors noted above.

DoIT operates largely on a fee-for-service basis, meaning that it charges State agencies for the services it provides to them. Therefore, reimbursable expenditures by DoIT increase by as much as $10.0 million annually beginning in fiscal 2023 as DoIT contractors perform the assessments for State agencies. State expenditures (all funds) and reimbursable revenues increase correspondingly as DoIT is reimbursed for its contract costs by State agencies.

Costs to State Agencies to Report Other Information

With one notable exception, each of the State agencies that replied to a request for information for the bill advises that it can provide the additional information to DoIT using existing resources or with minimal impact. However, the Department of Public Safety and Correctional Services (DPSCS) advises that it uses many disparate IT systems that do not communicate with each other, which makes gathering the necessary data for submission to DoIT more difficult. Therefore, in order to comply with the bill's requirements, DPSCS anticipates initial costs of approximately $1.2 million for additional staff, technology upgrades, and programming expenses, as well as ongoing operating expenses of approximately $200,000 a year.

However, given that all other State agencies indicate that they can comply with the bill's reporting requirements with existing resources, and that many agencies indicate that they already provide a lot of the information to DoIT, it is likely that DPSCS can satisfy the reporting requirement with existing resources. Therefore, this analysis does not reflect any such costs for DPSCS.

Local Expenditures: Local government expenditures increase, potentially significantly, beginning in fiscal 2023 as local governments obtain cybersecurity preparedness assessments and to the extent that IT systems must be modified to provide the required information to DoIT using DoIT's ITMP process. As noted above, private-sector costs for cybersecurity assessments range from tens of thousands to hundreds of thousands of dollars depending on the structure, complexity, and condition of a local agency's IT infrastructure. Since local governments do not have access to DoIT's third-party contracts, each local agency experiences costs within this range each year to obtain the assessments.

DoIT advises that some local governments may need to upgrade and/or consolidate their IT systems to ensure the required information can be transmitted to DoIT. Any such cost depends on each local agency's existing systems and practices, which is unknown, but the

costs could be significant for a local agency that uses older legacy systems or systems incompatible with DoIT's ITMP software.

Small Business Effect: Small businesses that offer cybersecurity preparedness assessments are likely to experience a significant increase in business under the bill.

Additional Information

Prior Introductions: None.

Designated Cross File: HB 587 (Delegate R. Watson) - Health and Government Operations.

Information Source(s): Department of Information Technology; Maryland Department of Aging; Department of Commerce; Comptroller's Office; Maryland State Treasurer's Office; Judiciary (Administrative Office of the Courts); Maryland State Department of Education; Baltimore City Community College; Maryland State Library Agency; University System of Maryland; Morgan State University; Maryland Department of Agriculture; Department of Budget and Management; Maryland Department of Disabilities; Department of General Services; Department of Housing and Community Development; Department of Human Services; Department of Juvenile Services; Department of Natural Resources; Maryland Department of Planning; Department of Public Safety and Correctional Services; Board of Public Works; Department of State Police; Maryland Department of Transportation; Department of Veterans Affairs; Maryland Insurance Administration; Baltimore, Montgomery, and Prince George's counties; Cybersecurity and Infrastructure Security Agency; Department of Legislative Services

Fiscal Note History: First Reader - March 8, 2021
rh/mcr

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.