Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 69 (Senators Hester and Simonaire)

Education, Health, and Environmental Affairs Health and Government Operations

Cybersecurity Coordination and Operations - Establishment and Reporting

This bill makes numerous changes to the State's cybersecurity infrastructure, practices, and procedures by (1) codifying and expanding the executive order that established the Maryland Cyber Defense Initiative; (2) requiring specified State and local governmental units that use the State-operated broadband network to certify that they comply with minimum cybersecurity requirements; and (3) requiring specified State and local governments to annually complete cybersecurity preparedness assessments and report specified information to the Department of Information Technology (DoIT) and/or the Governor, as specified.

Fiscal Summary

State Effect: General fund expenditures for DoIT increase by $1.2 million in FY 2022 for programming and 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 Executive Branch State agencies; State expenditures (all funds) and reimbursable revenues increase correspondingly as DoIT is repaid by those agencies for the assessments.

($ in millions)	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026
ReimB. Rev.	$10.0	$10.0	$10.0	$10.0	$10.0
GF Expenditure	$1.2	$1.3	$1.3	$1.4	$1.5
GF/SF/FF Exp.	$10.0	$10.0	$10.0	$10.0	$10.0
ReimB. Exp.	$10.0	$10.0	$10.0	$10.0	$10.0
Net Effect	($11.2)	($11.3)	($11.3)	($11.4)	($11.5)

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

Local Effect: Local government expenditures increase, potentially significantly, to obtain cybersecurity preparedness assessments and modify information technology (IT) processes and systems, if necessary, as discussed below. Revenues are not directly affected. **This bill imposes a mandate on a unit of local government.**

Small Business Effect: Meaningful.

Analysis

Bill Summary: Broadly, the bill expands the State's cybersecurity infrastructure in the following ways:

- codifies Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative, and expands and modifies the responsibilities of the various entities established by the executive order;
- requires specified State and local units of government that use the State-operated local access transport area (LATA) broadband network to annually certify to DoIT their compliance with minimum cybersecurity standards;
- requires each unit of State government in the Executive Branch to (1) complete annual cybersecurity preparedness assessments and report the results to the Office of Security Management (OSM) by December 1 each year; (2) report other specified IT and cybersecurity information to OSM and the Governor by December 1 each year; and (3) report cybersecurity incidents to the State Chief Information Security Officer (SCISO) in a specified manner; and
- requires each county government, school system, and local health department (excluding municipal governments) to (1) create or update a cybersecurity preparedness and response plan and submit the plan to OSM for approval by December each year; (2) complete annual cybersecurity preparedness assessments and report the results, and other specified IT and cybersecurity information, to OSM by December 1 each year; and (3) report cybersecurity incidents in a specified manner.

A more detailed description of these change can be found below.

Maryland Cyber Defense Initiative – Codified and Expanded

Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative, is codified and expanded. The initiative established OSM within DoIT; the position of SCISO to head OSM; and the Maryland Cybersecurity Coordinating Council (MCCC) to advise and assist SCISO and OSM. The bill adopts substantially similar responsibilities for

OSM, SCISO, and MCCC as those required by the executive order; however, the bill also expands the responsibilities beyond what is required by the executive order in the following ways:

- To the extent practicable, OSM must seek, identify, and inform relevant stakeholders of any available financial assistance provided by the federal government or non-State entities to support the work of OSM.
- OSM is responsible for the coordination of resources and efforts to implement cybersecurity best practices and improve overall cybersecurity preparedness and response for units of local government, local school boards, local school systems, and local health departments.
- OSM must review and certify local cybersecurity preparedness and response plans.
- OSM must (1) provide technical services, advice, and guidance to units of local government to improve cybersecurity preparedness, prevention, response, and recovery practices and (2) provide technical assistance to localities in mitigating and recovering from cybersecurity incidents.
- In coordination with the Maryland Emergency Management Agency (MEMA), OSM (1) must provide other types of assistance to local political subdivisions, related to cybersecurity preparedness and response plans and (2) may conduct regional exercises and establish regional assistance groups, as specified.
- By December 31 each year, OSM must provide an annual report to the Governor and specified committees of the General Assembly, that includes (1) OSM's activities and accomplishments from the previous 12 months and (2) a compilation and analysis of the data and information contained in cybersecurity reports received from State and local agencies, as specified.
- The membership of MCCC is expanded to include representatives from additional State agencies and offices, the University System of Maryland, the Legislative Branch of State government, and the Judicial Branch of State government.

To implement the existing and new responsibilities, the bill establishes two new positions (a director of State cybersecurity and a director of local cybersecurity) to oversee and implement the bill's requirements for units of State and local government, as appropriate. DoIT must provide OSM with sufficient staff to implement the bill, and OSM may procure resources, including regional coordinators, necessary to implement the bill.

State-operated LATA Broadband Network

By December 1 of each year, each unit of the Legislative and Judicial branches of State government, each unit of local government, and any local agencies that use the State-operated LATA broadband network must certify to DoIT that it is in compliance with DoIT's minimum cybersecurity standards.

State Cybersecurity Preparedness Assessments and Reporting

By December 1 each year, each unit of State government in the Executive Branch must (1) complete a cybersecurity preparedness assessment and report the results to OSM and (2) submit a report to the Governor and OSM that includes specified IT and cybersecurity information. The information that must be submitted includes an inventory of all information systems and applications used or maintained by the unit, the number of IT staff, including vacancies, and the unit's IT budget, itemized in a specified manner.

Each unit of State government in the Executive Branch must report a cybersecurity incident to SCISO. SCISO must determine (1) the criteria for determining when an incident must be reported; (2) the manner in which to report the incident; and (3) the time period in which to report.

Local Cybersecurity Preparedness Assessments and Reporting

By December 1 each year, each county government, local school system, and local health department must (1) consult with the local emergency manager to create or update a cybersecurity preparedness and response plan and submit the plan to OSM for approval; (2) complete a cybersecurity preparedness assessment and report the results to OSM, as specified; and (3) report specified IT and cybersecurity information to OSM, including the number of IT staff positions, including vacancies and the entity's cybersecurity budget.

Each county government, local school system, and local health department must report a cybersecurity incident to the appropriate local emergency manager. SCISO must determine (1) the criteria for determining when an incident must be reported; (2) the manner in which to report the incident; and (3) the time period in which to report.

Current Law:

Department of Information Technology and the Maryland Cyber Defense Initiative

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 Executive Order 01.01.2019.07, which created OSM, SCISO, and MCCC, and cybersecurity issues in the State and across the nation, please see the **Appendix – Cybersecurity**.

Maryland Emergency Management Agency and Gubernatorial Powers

MEMA, which is part of the Military Department, is responsible for coordinating the State response in any major emergency or disaster. This includes supporting local governments as needed or requested and coordinating assistance with the Federal Emergency Management Agency and other federal partners. MEMA manages many of the federal grants that fund a broad range of initiatives leading to enhanced protection from and responses to the full range of natural and man-made disasters that could threaten the State's citizens. Each local government has a Local Emergency Management Director who works with MEMA on behalf of the local government during a major emergency or disaster.

The Governor has control of and is responsible for MEMA and is responsible for carrying out the provisions of the Maryland Emergency Management Agency Act. In the event of the threat or occurrence of an emergency, the Governor may assume direct operational control over all or part of an emergency management function created or authorized by the Act. The Act enumerates specific powers the Governor has relating to emergency management. Among other things, if the Governor finds that an emergency has developed

or is impending due to any cause, the Governor must declare a state of emergency by executive order or proclamation.

State Expenditures:

Department of Information Technology – Staff and Reporting Costs and Savings

DoIT advises that it intends to implement the State and local government reporting aspects of 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 State and local cybersecurity oversight, as well as collecting, analyzing, and reporting IT and cybersecurity information. In addition to establishing a full office to oversee and assist with local government cybersecurity (including school boards and health departments), the bill requires DoIT to review and analyze cybersecurity assessments from all State Executive Branch agencies and specified local agencies, and to report the resulting information with greater specificity and granularity. In implementing the bill, DoIT plans to (1) modify its ITMP database application to accept the new information from State and local agencies; (2) replace its two contractors with eight permanent full-time staff to receive and analyze reports from State and local governments; and (3) establish an office with eight permanent full-time staff (including a local cybersecurity director) to assist and oversee local governments (totaling 16 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. DoIT can designate one of its existing staff as the State cybersecurity director.

Due to the bill's December 1 submission deadline for the IT/cybersecurity information and October 1, 2021 effective date, fiscal 2022 is the first year that State and local agencies must provide information to DoIT. For purposes of this analysis, it is assumed that each State and local agency receives a cybersecurity preparedness assessment and provides the required information to DoIT in that year; however, the Department of Legislative Services (DLS) notes that many agencies are unlikely to be able to meet the December 1, 2021 deadline. The estimate also assumes that the necessary programming costs for DoIT take place in fiscal 2022 and that staffing changes take place on October 1, 2021, so that the new staff can assist State and local agencies and begin their duties under the bill.

Thus, general fund expenditures for DoIT increase by $1.2 million in fiscal 2022. This estimate reflects the cost of hiring (1) eight full-time permanent program managers to handle report collection and analysis duties and (2) one local cybersecurity director, one grant coordinator, and six regional managers to handle local cybersecurity assistance and oversight duties. The estimate also reflects net savings of $250,000 in fiscal 2022 from one-time programming costs of $250,000, offset in part by savings of $500,000 from DoIT replacing the existing contractors that handle report collection and analysis duties. The estimate includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	16.0
Salaries and Fringe Benefits	$1,390,001
Programming Costs	250,000
Contractor Savings	-500,000
Operating Expenses	89,300
Total FY 2022 DoIT Expenditures	**$1,229,301**

Future year expenditures reflect full 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 – Executive Branch State Agencies

Some Executive Branch 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 Executive Branch 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. For purposes of this analysis, it is assumed that each State agency receives a cybersecurity assessment in fiscal 2022; however, some

agencies may not be able to provide the results to OSM by the December 1 deadline, since the bill takes effect on October 1, 2021.

Costs may vary to the extent that some Executive Branch 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 DLS 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 2022 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.

Reporting of Other Information

As noted above, DoIT plans to implement the bill by modifying the system it uses to annually collect MITDP information from State agencies. Since most or all State agencies already provide much of the information required by the bill to DoIT through this process, agencies can likely report any new information to DoIT at little to no additional cost.

State-operated LATA Broadband Network

The bill requires each unit of the Legislative and Judicial branches of State government that uses the State-operated LATA broadband network to annually certify to DoIT compliance with DoIT's minimum cybersecurity standards. The Judiciary advises it uses DoIT's LATA network and employs a rigorous cybersecurity framework based on National Institute of Standards and Technology best practices, which likely meets DoIT's standards. DLS advises that it and the General Assembly do not currently use DoIT's LATA network and, therefore, are unaffected by the bill. Even so, DLS and the General Assembly employ a rigorous cybersecurity framework that would likely meet DoIT's standards.

Local Expenditures: Local government expenditures increase, potentially significantly, beginning in fiscal 2022 as county governments, local school systems, and local health departments (1) develop, update and implement cybersecurity preparedness and response plans; (2) obtain cybersecurity preparedness assessments; and (3) to the extent necessary, modify their IT systems to provide the required information to DoIT using DoIT's ITMP process.

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. Additionally, any of the specified local government entities that does not currently maintain a cybersecurity preparedness and response plan is likely to experience costs to develop and implement a plan. 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 incompatible with modern cybersecurity practices or systems incompatible with DoIT's ITMP software.

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. It is unclear at this time whether local governments have access to DoIT's third-party contracts under the bill; for purposes of this analysis it is assumed that each local agency experiences costs within this range each year to obtain the assessments from the private sector.

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 879 (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; Military Department; Maryland Department of Transportation; Department of Veterans Affairs; Maryland Insurance Administration; Maryland Association of Counties; City of Salisbury; Maryland Municipal League; towns of Bel Air and Leonardtown; Baltimore, Montgomery, Prince George's, and Worcester counties; Cybersecurity and Infrastructure Security Agency; Department of Legislative Services

Fiscal Note History: First Reader - January 29, 2021
rh/mcr Third Reader - March 29, 2021
Revised - Amendment(s) - March 29, 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.