SB 811

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 811 (Senator Hester, *et al.*)

Budget and Taxation | Health and Government Operations and Appropriations

State Government - Information Technology and Cybersecurity-Related Infrastructure (Modernize Maryland Act of 2022)

This emergency bill establishes an independent Modernize Maryland Oversight Commission, expands cybersecurity requirements for State agencies and water and sewer systems, and makes related changes to cybersecurity infrastructure funding and procurement by the State and local governments. For fiscal 2023, funds from the Dedicated Purpose Account (DPA) may be transferred to implement the bill. For fiscal 2024, the Governor must include in the annual budget bill an appropriation of at least 20% of the amount appropriated for information technology (IT) and cybersecurity resources in the annual budget bill for fiscal 2023.

Fiscal Summary

State Effect: General fund expenditures increase by $10.1 million in FY 2023 for additional staff and for initial cybersecurity assessments for State agencies; $10.0 million is included in the FY 2023 budget for these assessments. Special fund expenditures from DPA are assumed to increase by $3.0 million in FY 2023 to capitalize and administer the Local Cybersecurity Support Fund. Future years reflect ongoing operating costs, capitalization for that fund (with general funds), and the mandated appropriation to DPA. Reimbursable revenues and expenditures increase by an estimated $10.0 million in FY 2026 for the next cybersecurity assessments; State agency expenditures (all funds) increase correspondingly. **This bill establishes a mandated appropriation for FY 2024.**

($ in millions)	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
SF Revenue	$3.0	$23.0	$3.0	$3.0	$3.0
ReimB. Rev.	$0	$0	$0	$10.0	$0
GF Expenditure	$10.1	$23.1	$3.1	$3.1	$3.1
SF Expenditure	$6.0	$23.0	$3.0	$3.0	$3.0
GF/SF/FF Exp.	$0	$0	$0	$10.0	$0
ReimB. Exp.	$0	$0	$0	$10.0	$0
Net Effect	($13.1)	($23.1)	($3.1)	($13.1)	($3.1)

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

Local Effect: Local revenues and expenditures for cybersecurity may increase significantly, as discussed below.

Small Business Effect: Meaningful.

Analysis

Bill Summary:

Modernize Maryland Oversight Commission

The independent Modernize Maryland Commission is established in the Department of Information Technology (DoIT) to (1) ensure the confidentiality, integrity, and availability of information held by the State concerning State residents and (2) advise the Secretary of Information Technology and the State Chief Information Security Officer (SCISO) on appropriate IT and cybersecurity investments and upgrades, funding sources, and future procurement mechanisms, as specified. The commission must:

- advise the Secretary of Information Technology on a strategic roadmap with a timeline and budget that will (1) require updates and investments of critical IT and cybersecurity systems, as specified, to be completed by December 31, 2025, as specified, and (2) require all updates and investments of IT and cybersecurity to be made by December 31, 2030;
- make periodic recommendations on investments in State IT structures based on the assessments required by the bill;
- review and provide recommendations on DoIT's basic security standards for use of the State's broadband network; and
- each year, report its findings and recommendations to specified committees of the General Assembly. (This report may not contain information about the security of an information system.)

Framework for Technology Investments and Cybersecurity Assessments

DoIT must hire independent contractors to develop a framework for investments in technology and, in accordance with the framework (at least once every three years), assess the cybersecurity and IT systems in each unit of State government. However, this requirement does not apply to (1) the Maryland Port Administration; (2) the University System of Maryland; (3) St. Mary's College of Maryland; (4) Morgan State University; (5) the Maryland Stadium Authority; (6) Baltimore City Community College; or (7) the State Board of Elections.

The framework must include specified criteria, and each affected unit of State government must promptly provide the contractors with the information necessary to perform the assessments. Every three years, the contractors must provide the results of the assessments to the Modernize Maryland Oversight Commission and specified committees of the General Assembly. The report may not contain information about the security of an information system.

DoIT may use multiple contractors at a time to meet these requirements.

Department of Information Technology – Responsibilities

The responsibilities of DoIT and the Secretary of Information Technology are expanded to include (1) upgrading IT and cybersecurity-related State government infrastructure and (2) annually evaluating specified technologies for providing public services and the development of data analytics capabilities to enable data-driven policymaking by units of State government.

Local Cybersecurity Support Fund

The Local Cybersecurity Support Fund is a special, nonlapsing fund that must be administered by the Secretary of Emergency Management. Its purpose is to provide financial assistance to local governments to improve cybersecurity preparedness, as specified, and assist local governments applying for federal cybersecurity preparedness grants. The fund may be used only (1) to provide financial assistance to local governments to improve cybersecurity preparedness, as specified; (2) to assist local governments applying for federal cybersecurity preparedness grants; and (3) for administrative expenses, as specified. Expenditures from the fund may only be made in accordance with the State budget.

To be eligible to receive assistance from the fund, a local government must (1) provide proof to DoIT that the local government conducted a cybersecurity preparedness assessment in the previous 12 months or (2) within 12 months, undergo a cybersecurity preparedness assessment, as specified.

Water and Sewer Systems

A public or private water or sewer system that serves a minimum of 10,000 users and receives financial assistance from the State must (1) assess its vulnerability to a cyber attack and (2) if appropriate, develop a cybersecurity plan. The Maryland Department of the Environment (MDE) may provide financial assistance to a public water or wastewater system to assess cybersecurity vulnerabilities and develop a cybersecurity plan.

Procurement

The authority of the Department of General Services (DGS) to engage in or control procurement is expanded to include, without the approval of any other primary procurement unit, (1) cloud computing equipment and associated services; (2) IT system modernization; and (3) cybersecurity upgrades and modernization.

Procurements by DGS for the purpose of modernizing cybersecurity infrastructure for the State valued below $1,000,000 are exempt from the Board of Public Works (BPW) oversight and approval. However, by December 1 of each year, DGS must submit a report to BPW on these procurements and include for each procurement (1) the purpose of the procurement; (2) the name of the contractor; (3) the contract amount; (4) the method of procurement utilized; (5) the number of bidders who bid on the procurement; and (6) the contract term.

Existing requirements that govern change orders for construction contracts are expanded to apply to State procurement contracts for information processing equipment and associated services and IT system and cybersecurity upgrades and modernization.

Current Law:

Department of Information Technology and Cybersecurity

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, as specified;
- adopting and enforcing nonvisual access standards to be used in the procurement of IT services, as specified;
- in consultation with the Attorney General, advising and overseeing a consistent cybersecurity strategy for units of State government, as specified;
- advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy; and
- in consultation with the Attorney General, developing guidance on consistent cybersecurity strategies for specified local government entities.

For information on recent cyberattacks affecting State agency and local government information systems and recent legislation and gubernatorial action taken to address cybersecurity and IT issues in the State, please see the **Appendix – Cybersecurity**.

Procurement and Change Orders

Chapter 590 of 2017 repealed the status of the Department of Budget and Management and DoIT as control and primary procurement units and transferred their authority to oversee procurements for IT, telecommunications, and services to DGS; current authorization for DGS to control procurement does not explicitly include cloud computing, IT modernization, or cybersecurity upgrades.

A "change order" is defined as a written order signed by a State procurement officer that directs a contractor to make changes that the contract authorizes the procurement officer to make without the consent of the contractor. A change order differs from a "contract modification," which changes the terms of a contract and requires mutual agreement by the parties. The following requirements apply to State procurement contracts for construction.

Generally, a unit of State government may not require a prime contractor to begin change order work under a contract until the procurement officer for the unit issues a written change order that specifies whether the work is to proceed in compliance with the terms of the contract, on an agreed-to price, force account, construction change directive, or time and materials basis. Similarly, a prime contractor cannot force a subcontractor to begin work unless the same conditions are met.

State Fiscal Effect:

Dedicated Purpose Account

DPA is one of four accounts that make up the State Reserve Fund, which is managed by the State Treasurer. The fiscal 2023 budget, as enacted, includes $100.0 million in DPA to address cybersecurity issues. Although the bill authorizes the use of funding in DPA to implement the bill, this analysis generally assumes DoIT uses that funding for other purposes related to cybersecurity. However, to the extent that DPA is used by DoIT to implement the bill, residual fiscal 2023 costs for DoIT may be partially or fully offset as this DPA funding is utilized. Further, as discussed below, this analysis assumes $3.0 million of that DPA funding is used to initially capitalize the Local Cybersecurity Support Fund.

Additionally, as noted above, the bill requires that the Governor include, for DPA, in the annual budget bill for fiscal 2024 not less than 20% of the aggregated amount appropriated for IT and cybersecurity resources in the fiscal 2023 budget bill. Accordingly, at least

$20.0 million must be provided in fiscal 2024. Thus, general fund expenditures increase by $20.0 million to appropriate the mandated funding to DPA, and special fund revenues and expenditures for the Treasurer increase correspondingly.

Department of Information Technology – Cybersecurity Assessments

The bill requires DoIT to engage contractors to perform cybersecurity assessments for State agencies at least once every three years. 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 the triennial assessments is approximately $10.0 million. The fiscal 2023 operating budget, as enacted, includes $10.0 million in general funds specifically for cybersecurity preparedness assessments as well as the $100.0 million in DPA noted above to address cybersecurity issues more broadly; this analysis assumes that the general funds are used for the cybersecurity preparedness assessments and that the assessments are undertaken and/or funded in fiscal 2023.

In fiscal 2026, however, reimbursable fund revenues and expenditures for DoIT increase by $10.0 million as cybersecurity assessments are once again performed pursuant to the bill's requirements. DoIT operates largely on a fee-for-service basis, meaning that it charges State agencies for the services it provides to them. State expenditures (all funds) and reimbursable revenues increase correspondingly as DoIT is reimbursed by agencies for conducting the cybersecurity assessments. To the extent that completion of the assessments is instead staggered over the next three years, expenditures are spread out over time.

Modernize Maryland Oversight Commission – Staff

General fund expenditures by DoIT also increase by $119,788 in fiscal 2023, which assumes a July 1, 2022 start date for staff due to the bill's emergency status. This estimate reflects the cost of hiring one cybersecurity policy and strategy planner to staff the Modernize Maryland Oversight Commission. It includes a salary, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Position	1.0
Salary and Fringe Benefits	$119,788
Operating Expenses	7,608
DoIT FY 2023 Personnel Expenditures	**$127,396**

Future year expenditures reflect annual increases and employee turnover as well as annual increases in ongoing operating expenses. DoIT may also incur additional costs to annually

evaluate new technologies for the delivery of public sector services in the manner required by the bill; however, any such costs are unknown and not included in this analysis.

Local Cybersecurity Support Fund

The bill establishes the Local Cybersecurity Support Fund within MDEM to provide financial assistance to local governments to improve cybersecurity preparedness and assist local governments applying for federal cybersecurity preparedness grants. The bill does not specify a funding source or funding amount for the fund, but the Department of Legislative Services notes that a significant amount of funding is likely required to support local cybersecurity efforts; IT and cybersecurity upgrades can be exceedingly costly depending on the work being done. As such, for purposes of this analysis, it is assumed that at least $3.0 million is needed annually for the fund to ensure an effective and viable program; however, the actual level of funding needed and provided may vary significantly. Based on the bill's authorization to transfer funds from DPA to implement the bill, it is assumed that, in fiscal 2023, the fund is capitalized using funds reserved in DPA. In the out-years, general funds are assumed to be used to maintain the fund.

MDEM needs additional staff to administer the fund. Therefore, special fund expenditures for MDEM increase by $189,988 in fiscal 2023, which assumes a July 1, 2022 start date for staff due to the bill's emergency status. This estimate reflects the cost of hiring two administrators to administer the Local Cybersecurity Support Fund. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	2.0
Salaries and Fringe Benefits	$174,772
Operating Expenses	15,216
MDEM FY 2023 Personnel Expenditures	**$189,988**

Future year expenditures reflect annual increases and employee turnover as well as annual increases in ongoing operating expenses. The bill authorizes the fund to be used to cover administrative expenses, so this analysis assumes that administrative costs are covered by the annual $3.0 million allocation to the fund, thereby reducing funds available for grants to local governments each year (approximately $2.8 million remains available for that purpose).

Local Fiscal Effect: Local revenues and expenditures increase significantly to the extent that a local government chooses to conduct a cybersecurity assessment in order to receive funding from the Local Cybersecurity Support Fund. Any specific impact on a local government depends on whether the government chooses to have an assessment and the amount of funding available and, therefore, cannot be reliably estimated at this time.

Locally owned water and sewer systems may experience additional costs to assess their vulnerability to cyber attacks and develop cybersecurity plans; however, any such impact cannot be reliably estimated at this time. To the extent that costs are incurred, they may be partially or fully offset by funding provided by MDE. Specifically, MDE advises that, while there is no specific funding available for this purpose, existing revolving loan funds could be used for this purpose.

Small Business Effect: Small businesses that offer cybersecurity preparedness assessments are likely to experience a significant increase in business under the bill. Additionally, privately owned water and sewer companies that qualify as small businesses may be affected in the same manner as local government water and sewer companies, as discussed above.

Additional Information

Prior Introductions: None.

Designated Cross File: HB 1205 (Delegate P. Young, *et al.*) - Health and Government Operations and Appropriations.

Information Source(s): Department of Information Technology; Maryland State Treasurer's Office; Department of Budget and Management; Department of General Services; Board of Public Works; Maryland Stadium Authority; Department of Legislative Services

Fiscal Note History: First Reader - February 20, 2022
rh/mcr Third Reader - April 11, 2022
Revised - Amendment(s) - April 11, 2022
Revised - Updated Information - April 11, 2022
Revised - Budget Information - April 11, 2022

Analysis by: Richard L. Duncan

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

Appendix – Cybersecurity

Cybersecurity Issues in the Nation and State

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, from 2019 through 2021, the Center for Strategic and International Studies identified over 300 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.

Maryland governmental entities have often been the victim of significant cyberattacks in recent years. For example:

- in 2019, (1) Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks and (2) the Maryland Department of Labor's licensing database was breached; the personal identifiable information (PII) of as many as 78,000 licensees may have been accessed by the hackers;
- in November 2020, Baltimore County Public Schools' information technology (IT) systems were made unusable by a ransomware attack; and
- in 2021, (1) multiple southern Maryland towns lost computer access after a third-party vendor was the victim of a ransomware attack and (2) the Maryland Department of Health was the victim of a cyberattack, resulting in the delay of pandemic data and other information.

Additionally, in November 2021, the Virginia Legislature was the victim of a ransomware attack.

Cybersecurity Governance – Generally

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.

Recent State Action

During the 2021 legislative session, multiple pieces of legislation were enacted to enhance State cybersecurity and resilience.

- Chapter 218 of 2021 requires the Secretary of Information Technology to consult with the Attorney General to oversee a consistent cybersecurity strategy specifically for the Executive Branch.
- Chapter 683 of 2021 establishes the Center for Cybersecurity at the University of Maryland Baltimore County in order to provide research and support for cybersecurity-related activities.
- Chapter 425 of 2021 expands the list of network-related prohibited acts on a broad array of computer networks in the State. Chapter 425 also prohibits a person from performing acts to impair network functioning, including exceeding authorized network access and distributing valid access codes to unauthorized persons, on public school or health care facility networks.

In July 2021, the Governor announced several new cybersecurity measures that his office will be undertaking, including (1) a new partnership with the National Security Agency; (2) a memorandum of understanding with the University of Maryland Baltimore County to establish the Maryland Institute of Innovative Computing; and (3) an executive order creating a statewide privacy framework to govern the manner in which the State secures the PII of its citizens.

Maryland Cybersecurity Council Study

The Maryland Cybersecurity Council is required to work with the National Institute of Standards and Technology, as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State cybersecurity issues. Over the 2021 interim, a council workgroup conducted a review and study of the State's cybersecurity governance and resilience. Through the study, the workgroup developed numerous recommendations for the State to improve and enhance its system. The recommendations include codifying the aforementioned executive order that established the Maryland Cyber Defense Initiative

and centralizing State cybersecurity and IT governance within DoIT. The workgroup's final report is expected to be released during the 2022 legislative session.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures advises that 45 states, the District of Columbia, and Puerto Rico introduced or considered over 250 bills or resolutions that dealt significantly with cybersecurity in 2021. Some of the key cybersecurity issues considered included:

- requiring government agencies to implement training or specific types of security policies and practices and improving incident 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.

Federal Action

On October 8, 2021, President Joseph R. Biden, Jr., signed the K-12 Cybersecurity Act into law in response to cybersecurity attacks directed at schools. Narrow in scope, the law directs the federal Cybersecurity and Infrastructure Security Agency (CISA) to examine cybersecurity-related risks exclusive to K-12 educational settings. The Director of Cybersecurity and Infrastructure Security must conduct a study and make recommendations specific to K-12 related cybersecurity risks.

Additionally, the Infrastructure Investment and Jobs Act was signed into law on November 15, 2021. Related to cybersecurity, the act established a cyber grant program within the Federal Emergency Management Agency that must be managed in consultation with CISA. Through the program, $1 billion will be distributed to state and local governments over four years; however, to receive a grant, states must submit a cybersecurity plan to the Department of Homeland Security, establish a planning committee before grants are received, and match a portion of the funding provided over the grant program. Grant funding may not be used for ransomware attack payments, to supplant other funding, or for any noncyber purpose.