SB 780

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 780 (Senator Hester)

Education, Health, and Environmental Affairs and Budget and Taxation

Cybersecurity Governance Act of 2022

This bill significantly expands and enhances the State's regulatory framework related to cybersecurity for State and local governments. Among other things, the bill (1) centralizes the governance of information technology (IT) and cybersecurity for all units of the Executive Branch of State government in the Department of Information Technology (DoIT); (2) codifies and expands the Maryland Cyber Defense Initiative; (3) requires all State agencies, and certain local government entities, to obtain annual cybersecurity assessments; (4) establishes multiple reporting requirements for State agencies and local governments; and (5) establishes new offices to assist local governments with cybersecurity preparedness. The Governor must include an appropriation in the annual budget in an amount necessary to cover the costs of implementing the statewide cybersecurity master plan required by the bill.

Fiscal Summary

State Effect: General fund expenditures increase by *at least* $17.7 million in FY 2023 for DoIT and Maryland Department of Emergency Management (MDEM) staff and operating costs and for cybersecurity assessments; future years reflect annualization and ongoing costs. State expenditures (all funds) likely increase significantly across all agencies due to the bill's centralization of IT and cybersecurity in DoIT, to implement the cybersecurity master plan, and to produce the various required reports; this impact is not shown below. Revenues are not likely affected.

($ in millions)	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
Revenues	$0	$0	$0	$0	$0
GF Expenditure	17.7	19.0	19.2	19.4	19.6
GF/SF/FF Exp.	-	-	-	-	-
Net Effect	($17.7)	($19.0)	($19.2)	($19.4)	($19.6)

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

Local Effect: County and Baltimore City expenditures increase, potentially significantly, to obtain annual cybersecurity assessments and produce the required plans and reports. Revenues may be affected, as discussed below. **This bill may impose a mandate on a unit of local government.**

Small Business Effect: Meaningful.

Analysis

Bill Summary: Broadly, the bill:

- centralizes the governance of IT and cybersecurity for all units of the Executive Branch of State government in DoIT (including transferring all IT funding, records, and property from Executive Branch agencies to DoIT and requiring IT staff in Executive Branch agencies to report to the Secretary of Information Technology);
- codifies various aspects of Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative, the Office of Security Management (OSM), and the Maryland Cybersecurity Coordinating Council (MCCC) in DoIT, and expands and modifies OSM's and MCCC's responsibilities;
- requires the Governor to report to the General Assembly by January 31 of each year on specified IT and cybersecurity issues and funding;
- requires DoIT to address preparedness and response capabilities of local jurisdictions and coordinate the procurement of managed cybersecurity services procured by local governments with State funding;
- requires DoIT to develop and require basic security requirements that include specified criteria to be included in State contracts in which a third-party contractor will have access to and use State telecommunications equipment, systems, or services;
- expands DoIT's responsibilities to include (1) centralizing the management and direction of IT within the Executive Branch under the control of DoIT; (2) providing or coordinating the procurement of managed cybersecurity services that are paid for by the State and used by local governments; and (3) developing a statewide cybersecurity master plan, as specified;
- requires the Chair of the Maryland Cybersecurity Council (MCC) to appoint a cybersecurity master plan subcommittee of the council to provide advice to the Secretary of Information Technology on the creation of the cybersecurity master plan;

- requires specified State and local units of government that use the State-operated broadband network to annually certify to DoIT their compliance with minimum cybersecurity standards;
- requires each unit of State government, by December 1 of each year, to complete a cybersecurity preparedness assessment and report the results to OSM, as specified;
- requires each unit of State government to obtain an external vulnerability and risk assessment at least once every two years, report the results to OSM, and report to OSM when any subsequent remediation takes place;
- requires each unit of State government, by December 1 of each year, to report to the Governor and General Assembly on specified information related to IT equipment, initiatives, and staffing;
- requires each unit of State government to report a cybersecurity incident to the State Chief Information Security Officer (SCISO), who must then take specified actions;
- requires specified local government entities (but not municipal governments) to annually develop cybersecurity-related plans, complete cybersecurity preparedness assessments, and report specified information to OSM;
- expands the authority of the Department of General Services (DGS) to include the procurement of managed cybersecurity services;
- requires DoIT, by December 31, 2022, to complete the implementation of a governance, risk, and compliance (GRC) module across the Executive Branch of State government that meets specified requirements; and
- requires the State Chief Data Officer, by December 31, 2023, to contract with an independent third party to work with specified State entities to develop a statewide reporting framework based on the Cybersecurity Framework developed by the National Institute of Standards and Technology and that meets specified requirements.

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

Information Technology and Cybersecurity Governance

On the bill's effective date, (1) all appropriations held by a unit of the Executive Branch of State government for the purpose of IT operations or cybersecurity are transferred to DoIT; (2) all books and records, real and personal property, equipment, fixtures, assets, liabilities, obligations, credits, rights, and privileges held by a unit of the Executive Branch of State government for the purpose of IT operations or cybersecurity are transferred to DoIT; and (3) all employees of a unit of the Executive Branch of State government who are assigned more than 50% of the time to a function related to IT operations and cybersecurity report to the Secretary of Information Technology or the Secretary's designee.

The bill includes other provisions to ensure the efficient transfer of, among other things, contracts, property, and responsibilities from Executive Branch agencies to DoIT, and makes a series of conforming changes.

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 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:

- SCISO must be appointed by the Governor with the advice and consent of the Senate.
- OSM must coordinate resources and efforts to implement cybersecurity best practices and improve cybersecurity preparedness and response for specified local government entities.
- OSM must establish standards to categorize all information collected or maintained by or on behalf of each unit of State government.
- OSM must develop and maintain IT security policies, standards, and guidance documents, consistent with best practices developed by the National Institute of Standards and Technology.
- OSM must conduct an annual cybersecurity survey of all units of State government.
- OSM must ensure each unit of State government receives an external vulnerability assessment at least once every two years, receive reports on vulnerabilities and high-risk configurations identified in the assessment, and assist any unit in necessary remediation identified in the assessment.
- OSM must, to the extent practicable, 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 the office.
- OSM must (1) review and certify local cybersecurity and preparedness and response plans; (2) provide technical assistance to localities in mitigating and recovering from cybersecurity incidents; and (3) provide technical services, advice, and guidance to units of local government to improve cybersecurity preparedness, prevention, response, and recovery practices.

- OSM must coordinate with MDEM to assist specified local government entities with specified cybersecurity issues.
- OSM may coordinate with MDEM to 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 specified information.
- The membership of MCCC is expanded and its responsibilities are expanded to include review of OSM analyses to develop recommendations, as specified.

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.

Local Cybersecurity Preparedness Assessments and Reporting

The following requirements do not apply to municipal governments. 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.

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, MCCC, and recent legislation and gubernatorial action taken to address cybersecurity and IT issues in the State, please see the **Appendix – Cybersecurity**.

Maryland Department of Emergency Management

Chapters 287 and 288 of 2021 established MDEM as a principal department of the Executive Branch of State government and as the successor to the Maryland Emergency Management Agency. MDEM 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. MDEM 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 MDEM on behalf of the local government during a major emergency or disaster.

State Fiscal Effect:

Transfer of Information Technology and Cybersecurity Governance to the Department of Information Technology

As noted above, on October 1, 2022, the bill centralizes the governance of IT and cybersecurity for all units of the Executive Branch of State government in DoIT (including requiring IT staff to report to the Secretary of Information Technology). For purposes of this analysis, it is assumed that existing staff remain in the agencies where they currently reside to provide ongoing direct technical support to the agencies. This is similar to the manner in which the Attorney General's Office provides legal support and guidance to each State agency.

The bill does not authorize or require the actual transfer of staff positions to DoIT, so this analysis does not assume any transfer of compensation linked to those positions. However,

the bill does require the transfer of other appropriations for IT operations or cybersecurity. Therefore, State expenditures (all funds) for State agencies decrease significantly, and general fund expenditures for DoIT increase significantly beginning in fiscal 2023. The bill's transfer of appropriations and property likely reflect hundreds of millions of dollars, or more, and may take many years to complete. DoIT advises that it took five years to centralize IT for the 30 agencies for which it provides full IT services.

In the short-term, there is most likely to be a potentially significant net increase in spending as new processes and procedures are established and redundancies are identified and eliminated. However, over time, DoIT is likely to be able to provide services more efficiently to State agencies through the centralized system, resulting in potentially significant net cost savings for IT and cybersecurity in future fiscal years.

There may be significant operational issues with the bill's centralization of IT and cybersecurity governance. For example, the Department of State Police advises that DoIT may not have authority to access the federal crime databases that it uses for its operations.

Department of Information Technology

In addition to the acquisition of IT staff and resources discussed above, DoIT requires additional staff to handle the substantial additional responsibilities required by the bill. Because the bill requires DoIT to provide OSM with sufficient resources and staff to implement the bill, including the procurement of resources, including regional coordinators, DoIT estimates that 42 additional staff are needed. Additionally, DoIT incurs additional annual contractual costs to license vulnerability assessment software and to implement a GRC module across all State agencies.

The bill also requires each State agency, by December 1 of each year, to obtain a cybersecurity preparedness assessment. DoIT advises that, on average, cybersecurity assessments of the kind required by the bill cost between $75,000 and $100,000 per IT system, and the State has approximately 125 different systems spanning all Executive Branch agencies. As such, the total cost of conducting the assessments for each State agency is approximately $10.0 million annually. Since the bill transfers all IT and cybersecurity governance to DoIT, this estimate assumes that DoIT pays these costs directly and does not charge State agencies for the assessment. The Governor's proposed fiscal 2023 operating budget, as introduced, includes $10 million for cybersecurity assessments; this analysis assumes that those funds are used for this purpose in fiscal 2023.

Therefore, general fund expenditures by DoIT increase by $17.3 million in fiscal 2023, which accounts for the bill's October 1, 2022 effective date. This estimate reflects the cost of hiring 42 full-time staff, including cyber policy and strategy planners, cyber defense incident responders, and vulnerability assessment analysts to handle the significant

expansion of responsibilities for OSM, including providing significant levels of assistance to local governments. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses. It also includes $10 million for cybersecurity assessments, $1 million for external vulnerability assessment software, and $1 million to implement the GRC module.

Positions	42
Salaries and Fringe Benefits	$5,036,967
Cybersecurity Assessments	10,000,000
Vulnerability Assessment Software	1,000,000
GRC Module Costs	1,000,000
Operating Expenses	308,406
Total FY 2023 DoIT Expenditures	**$17,345,373**

Future year expenditures reflect annualization and full salaries with annual increases and employee turnover, annual increases in ongoing operating expenses, ongoing licensing costs for the vulnerability assessment and GRC software, and ongoing costs for State agency cybersecurity assessments.

DoIT anticipates significant additional costs in future fiscal years to implement the statewide cybersecurity master plan and may incur potentially significant costs depending on the disposition of the external vulnerability assessments; however, any such impact depends on the ultimate disposition of the plan and cannot be reliably estimated at this time. A reliable estimate of the cost of contracting with an independent third party to develop a statewide reporting framework is not available as it is currently outside of DoIT's responsibilities; therefore, this estimate does not include an estimate of its cost, but it may be significant.

Maryland Department of Emergency Management

MDEM advises that its Cyber Preparedness Unit currently supports local governments in preparedness activities for cyber events, including planning, training, and exercises. However, the bill expands its responsibilities to include assisting school systems and local health departments and to provide assistance on a broader array of cybersecurity issues for which MDEM requires additional staff. Therefore, general fund expenditures by MDEM increase by $393,835 in fiscal 2023, which accounts for the bill's October 1, 2022 effective date. This estimate reflects the cost of hiring five full-time staff and one half-time staff for the unit, including planning specialists, training and exercise specialists, a school system coordinator, and a half-time human resources officer. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	5.5
Salaries and Fringe Benefits	$350,174
Operating Expenses	43,661
Total FY 2023 MDEM Expenditures	**$393,835**

Future year expenditures reflect annualization and full salaries with annual increases and employee turnover as well as annual increases in ongoing operating expenses.

State-operated Broadband Network

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

Procurement

Although the bill expands DoIT's authorities related to the acquisition of IT and procurement on behalf of local governments, the bill maintains DGS's control over the procurement of IT and expands its responsibilities to include control of procurement for cybersecurity services. Thus, this estimate assumes that DGS continues to be the primary procurement agency for IT and cybersecurity issues for State agencies.

Local Fiscal Effect: Local expenditures increase, potentially significantly, beginning in fiscal 2023 as county governments, local school systems, and local health departments (1) develop, update, and implement cybersecurity preparedness and response plans and (2) conduct annual cybersecurity preparedness assessments.

The total cost for each affected local government cannot be reliably estimated at this time, as it primarily depends on (1) how many IT systems must be assessed for each local government and (2) the complexity of the systems being assessed. Specifically, private-sector costs for cybersecurity assessments range significantly depending on the type of assessment being done and the size and complexity of the IT system being assessed; costs can range from between $15,000 (for basic assessments and systems) and $100,000 (for more complicated assessments and systems). As noted above, costs for the high-quality assessments used by DoIT generally range from $75,000 to $100,000 per system.

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: None.

Information Source(s): Department of Information Technology; Maryland Department of Emergency Management; Maryland Department of Agriculture; Department of Commerce; Department of Natural Resources; Maryland Department of Planning; Maryland State Department of Education; Maryland Department of the Environment; Department of General Services; Department of Housing and Community Development; Maryland Department of Disabilities; Maryland Department of Health; Judiciary (Administrative Office of the Courts); Maryland Association of Counties; Maryland Association of County Health Officers; Military Department; Department of State Police; Maryland Department of Aging; Office of the Public Defender; State Prosecutor's Office; Department of Public Safety and Correctional Services; Maryland Department of Transportation; University System of Maryland; Department of Veterans Affairs; Maryland Association of Counties; Charles, Frederick, Montgomery, and Somerset counties; Maryland Municipal League; Department of Legislative Services

Fiscal Note History: First Reader - March 2, 2022
fnu2/mcr

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.