HB 1202

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
Enrolled - Revised

House Bill 1202 (Delegate P. Young, *et al.*)
Health and Government Operations Education, Health, and Environmental Affairs

Local Government Cybersecurity - Coordination and Operations (Local Cybersecurity Support Act of 2022)

This emergency bill makes numerous changes to the State's cybersecurity infrastructure, practices, and procedures, primarily for local governments, by, among other things, (1) codifying (in part) and expanding the executive order that established the Maryland Cyber Defense Imitative; (2) establishing the Cybersecurity Preparedness Unit in the Maryland Department of Emergency Management (MDEM) and the Information Sharing and Analysis Center (ISAC) within the Department of Information Technology (DoIT); (3) requiring specified local government entities to create or update cybersecurity preparedness and response plans and complete cybersecurity preparedness assessments, as specified; and (4) requiring DoIT to provide guidance to local governments to bring their cybersecurity practices into compliance with cybersecurity standards. For fiscal 2023, funds from the Dedicated Purpose Account (DPA) may be transferred by budget amendment to implement the bill. Beginning in fiscal 2024, the Governor must include in the annual budget bill specified funding for staff for the Cybersecurity Preparedness Unit.

Fiscal Summary

State Effect: General fund expenditures increase by an estimated $6.5 million in FY 2023 for MDEM and DoIT staff and study costs. Future years reflect ongoing staff and operating costs. State expenditures (all funds) and reimbursable revenues increase significantly and correspondingly as DoIT provides services to State agencies and is paid by those agencies using its fee-for-service model. Reimbursable expenditures increase correspondingly to offset some of DoIT's costs. **This bill establishes a mandated appropriation beginning in FY 2024.**

($ in millions)	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
ReimB. Rev.	-	-	-	-	-
GF Expenditure	$6.5	$7.8	$7.9	$8.1	$8.3
GF/SF/FF Exp.	-	-	-	-	-
Net Effect	($6.5)	($7.8)	($7.9)	($8.1)	($8.3)

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, as discussed below. These costs may be offset to the extent that local governments receive assistance from DoIT and MDEM, 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:

- codifies aspects of Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative and the Office of Security Management (OSM) in DoIT, and expands and modifies OSM's responsibilities;
- clarifies that existing requirements related to major information technology (IT) development projects apply to cybersecurity projects as well;
- requires DoIT to provide guidance for local government cybersecurity under certain circumstances;
- requires the State Chief Information Security Officer (SCISO) to establish guidelines by October 1, 2022, for when a cybersecurity incident must be disclosed to the public, and complete and submit a related report on the guidelines by November 1, 2022, as specified;
- establishes qualifications for the SCISO;
- requires that, for fiscal 2024 and each fiscal year thereafter, the Governor must include in the annual budget bill a specified appropriation for five positions for the Cyber Preparedness Unit;
- in a manner and frequency established in regulations adopted by DoIT, requires each unit of local government and local agencies that use the State-operated broadband network to annually certify to DoIT their compliance with minimum cybersecurity standards;
- requires specified local government entities (but not municipal governments) to, in a manner and frequency established in regulations adopted by DoIT, develop cybersecurity preparedness and response plans and complete cybersecurity preparedness assessments;
- authorizes DoIT to establish a program that leverages State purchasing power to offer favorable rates to units of local government to procure IT or cybersecurity services from contractors; however, a unit of local government is not required to participate in such a program;
- requires local government entities to report a cybersecurity incident to specified entities;

- specifies that the Office of Legislative Audits must redact any cybersecurity findings in a manner consistent with auditing best practices before an audit report is made available to the public;
- requires the SCISO and Secretary of Emergency Management to complete a budget review, make recommendations, and establish guidance related to cybersecurity preparedness by December 1, 2022, as specified; and
- requires the SCISO to complete a feasibility study on expanding the operations of the Security Operations Center operated by DoIT to include cybersecurity monitoring and alert services for units of local government and report its recommendation to the Governor and General Assembly by December 1, 2023; for fiscal 2024, the Governor must include an appropriation in the annual budget to cover the cost of the study.

A more detailed description of these changes 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, in part, and expanded. Specifically, the bill codifies the establishment of OSM within DoIT and the position of the SCISO to head OSM. The bill does not include any reference to the Maryland Cybersecurity Coordinating Council (which was also established by the executive order). The bill adopts substantially similar responsibilities for OSM and the SCISO; however, the bill also alters and expands the responsibilities beyond what is required by the executive order in the following ways:

- The SCISO must be appointed by the Governor with the advice and consent of the Senate and meet the education and experience qualifications specified by the bill.
- OSM is responsible for working with the MDEM Cyber Preparedness Unit during emergency response efforts, as specified.
- If the SCISO determines that there are security vulnerabilities or deficiencies in any information systems, the OSM must determine and direct or take actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected.
- If the SCISO determines that there is a cybersecurity threat caused by an entity connected to the State broadband network that introduces a serious risk to entities connected to the network or the State, OSM must take or direct actions required to mitigate the threat.
- OSM is not responsible for IT information installation and maintenance operations normally conducted by a unit of State government, a unit of local government, a local school board, a local school system, or a local health department.

- 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, 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) provide technical assistance to localities in mitigating and recovering from cybersecurity incidents and (2) 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 preparedness plans and related activities.
- 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, which 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. (A report may not contain information that reveals cybersecurity vulnerabilities and risks to the State.)

To implement the existing and new responsibilities, the bill establishes two new positions (a director of State cybersecurity and a director of local cybersecurity) within OSM 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.

Information Sharing and Analysis Center

ISAC must (1) coordinate information on cybersecurity by serving as a central location for information sharing across State and local government, federal government partners, and private entities; (2) with OSM, support cybersecurity coordination between local units of government through existing local government stakeholder organizations; (3) provide support to the SCISO and Cyber Preparedness Unit during cybersecurity incidents that affect State and local governments; (4) support risk-based planning for the use of federal resources; and (5) conduct analyses of cybersecurity incidents.

Cyber Preparedness Unit and Reporting of Cybersecurity Incidents

In coordination with the SCISO, the Cyber Preparedness Unit must (1) support local governments in developing a vulnerability assessment and cyber assessment, as specified; (2) develop and regularly update an online database of cybersecurity training resources for

local government personnel, as specified; (3) assist local governments in the development of cybersecurity preparedness and response plans, implementing best practices and guidance developed by the SCISO, and identifying and acquiring resources to complete appropriate cybersecurity vulnerability assessments; (4) connect local governments to appropriate resources for any other purpose related to cybersecurity, as specified; (5) conduct regional cybersecurity preparedness exercises, as necessary and specified; and (6) establish regional assistance groups to deliver and coordinate support services to local governments, agencies, or regions. The unit must also support OSM during emergency response efforts.

The bill requires five position identification numbers to be created for the purpose of hiring staff to conduct the duties of the Cybersecurity Preparedness Unit and mandates that the Governor include at least $357,978 in the annual budget bill for those positions, beginning in fiscal 2024.

Each local government must report a cybersecurity incident, including an attack on a State system being used by the local government, to the appropriate local emergency manager, the State Security Operations Center in DoIT, and the Maryland Joint Operations Center in MDEM. The SCISO must determine the criteria for when an incident must be reported, the manner in which to report, and the time period within which a report must be made. The State Security Operations Center must immediately notify appropriate agencies of a reported incident.

Local Cybersecurity Preparedness Assessments and Reporting

The following requirements do not apply to municipal governments. In a manner and frequency established in regulations adopted by DoIT, 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 (2) complete a cybersecurity preparedness assessment.

Local Government Certification

By June 30, 2023, each unit of local government must certify to OSM its compliance with State minimum cybersecurity standards established by DoIT. Certification must be reviewed by independent auditors, and any findings must be remediated. If a unit of local government has not remediated any such findings by July 1, 2024, OSM must provide guidance for the unit to achieve compliance with the cybersecurity standards.

Budget Review and Incident Reporting

By December 1, 2022, the SCISO and Secretary of Emergency Management must (1) review the State budget for efficiency and effectiveness of funding and resources to ensure that the State is equipped to respond to a cybersecurity attack; (2) make recommendations for any changes to the budget needed to accomplish those goals; (3) establish guidance for units of State government on use and access to State funding related to cybersecurity preparedness; and (4) report any recommendations and guidance to the Governor and General Assembly.

By October 1, 2022, the SCISO must establish guidelines to determine when a cybersecurity incident must be disclosed to the public. By November 1, 2022, the SCISO must submit a report on the guidelines to the Governor and specified committees of the General Assembly.

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 cyber-attacks affecting State agency and local government information systems and recent legislation and gubernatorial action taken to address cybersecurity and IT issues in the State, including the Governor's Cyber Defense Initiative, 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:

Dedicated Purpose Account

DPA is one of four accounts that make up the State Reserve Fund. The fiscal 2023 budget, as enacted, includes $200 million in DPA to address cybersecurity issues – $100.0 million as a deficiency appropriation for fiscal 2022 and another $100.0 million for fiscal 2023. Also, DPA has $10.0 million in unexpended funds from fiscal 2021 specifically for cybersecurity assessments; this $10.0 million in funding will expire at the end of fiscal 2025. Although the bill authorizes the use of funding in DPA to implement the bill in fiscal 2023, this analysis *generally* assumes that DoIT uses DPA funding for other purposes related to cybersecurity (such as upgrading existing systems). To the extent that the funding in DPA can be used to implement the bill, fiscal 2023 costs may be partially or fully offset by those funds.

Department of Information Technology and State Costs

To handle the substantial additional responsibilities required by the bill, and because the bill requires DoIT to provide OSM with sufficient resources and staff to implement the bill, DoIT requires 40 additional staff. Additionally, DoIT incurs additional contractual costs to purchase vulnerability assessment software.

Therefore, general fund expenditures by DoIT increase by $6.1 million in fiscal 2023, which assumes an October 1, 2022 start date for staff. This estimate reflects the cost of hiring 40 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 $1 million for vulnerability assessment

software. This estimate assumes that DoIT's new staff can handle the bill's required budget review, feasibility study, and incident report. The estimate reflects a robust and thorough implementation of the bill.

Positions	40.0
Salaries and Fringe Benefits	$4,790,260
Vulnerability Assessment Software	1,000,000
Operating Expenses	293,720
Total FY 2023 DoIT Expenditures	**$6,083,980**

Future year expenditures reflect full salaries with annual increases and employee turnover as well as annual increases in ongoing operating expenses and ongoing licensing costs for the vulnerability assessment software.

State expenditures (all funds) and reimbursable revenues increase significantly and correspondingly as DoIT provides services to State agencies under the bill's requirements and charges those agencies using its fee-for-service model. Additionally, reimbursable expenditures offset some of DoIT's aforementioned costs.

Maryland Department of Emergency Management – Staffing Costs

MDEM advises that it has recently implemented a Cyber Preparedness Unit but does not currently have sufficient staff to handle the additional responsibilities required by the bill for the Unit. Moreover, to fulfill these additional responsibilities, MDEM needs more than the five positions mandated by the bill for the unit. Therefore, general fund expenditures by MDEM increase by $454,857 in fiscal 2023. This estimate assumes an October 1, 2022 start date for staff. It reflects the cost of hiring six full-time staff and one half-time staff, including liaisons, coordinators, and officers to directly assist local governments and develop and update guidance, trainings, and best practices. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	6.5
Salaries and Fringe Benefits	$403,853
Operating Expenses	51,004
Total FY 2023 MDEM Expenditures	**$454,857**

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

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;

(2) conduct annual cybersecurity preparedness assessments; and (3) obtain audits of their IT systems.

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 vary 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) to $100,000 (for more complicated assessments and systems).

Local government costs for plan implementation and cybersecurity assessments may be offset to the extent that they receive assistance from MDEM and DoIT in the manner required by the bill; however, any such offset cannot be reliably estimated without actual experience under the bill.

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: SB 754 (Senator Hester, *et al.*) - Education, Health, and Environmental Affairs.

Information Source(s): Department of Information Technology; Maryland Department of Emergency Management; Office of the Public Defender; State Prosecutor's Office; Register of Wills; Department of Budget and Management; Judiciary (Administrative Office of the Courts); Maryland Association of Counties; Maryland Municipal League; Maryland Association of County Health Officers; Carroll, Harford, Montgomery, and St. Mary's counties; Office of Legislative Audits; Department of Legislative Services

Fiscal Note History: First Reader - February 20, 2022
rh/mcr Third Reader - March 24, 2022
Revised - Amendment(s) - March 24, 2022
Enrolled – May 10, 2022
Revised - Amendment(s) – May 10, 2022
Revised - Budget Information – May 10, 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 the 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.