Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 5 (Delegate Krimm)
Health and Government Operations

State Government - State and Local Government Employees and Contractors - Cybersecurity Training

This bill generally applies existing requirements related to the protection of personal information to the Legislative and Judicial branches of State government. The bill also requires the Maryland Cybersecurity Coordinating Council (MCCC) to develop a Cybersecurity Awareness and Training Program to certify training programs, as specified; beginning on October 1, 2023, certain State and local employees must complete a certified cybersecurity training at least *four times per year* and certain government contractors must receive training as well. By April 1, 2023, MCCC must develop standards for the program and trainings. **The bill applies prospectively and may not be applied or interpreted to have any effect on or application to any contract executed before the bill's October 1, 2022 effective date.**

Fiscal Summary

State Effect: Even though most State employees receive cybersecurity training under current practices, State expenditures (all funds) may increase for training and administrative costs, as discussed below. General fund expenditures by the Department of Information Technology (DoIT) increase by $937,500 annually beginning in FY 2024 to administer the training program. Reimbursable expenditures and revenues for DoIT increase by $225,000 annually beginning in FY 2024.

(in dollars)	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
ReimB. Rev.	$0	$225,000	$225,000	$225,000	$225,000
GF Expenditure	0	937,500	937,500	937,500	937,500
GF/SF/FF Exp.	0	-	-	-	-
ReimB. Exp.	0	$225,000	$225,000	$225,000	$225,000
Net Effect	$0	(-)	(-)	(-)	(-)

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

Local Effect: Local government expenditures increase, in some cases potentially significantly, for cybersecurity training, administrative costs, and contract costs. **This bill may impose a mandate on a unit of local government.**

Small Business Effect: Potential meaningful.

Analysis

Bill Summary:

Cybersecurity Awareness and Training Program

MCCC must develop a Cybersecurity Awareness and Training Program that includes a course of periodic cybersecurity training activities, each of which includes audits of the cybersecurity trainings. The State Chief Information Security Officer (SCISO) must coordinate with MCCC to annually certify trainings for use under the program and update standards for the maintenance of cybersecurity trainings. MCCC must determine the number of trainings to be certified and provide minimum standards for the training content. The bill establishes criteria that MCCC must use for the certification process. The SCISO may contract with a third party to certify the trainings.

Beginning October 1, 2023, MCCC must annually publish a list of the certified trainings on DoIT's website.

Cybersecurity Training Requirements for State and Local Employees

Beginning October 1, 2023, each State and local employee (including employees of the Legislative and Judicial Branches of State government) must complete a certified cybersecurity training if that employee's job duties include accessing a State or local government computer system or database. MCCC must ensure that each employee completes a training *at least four times* each year. A governmental unit may require other employees to complete cybersecurity trainings as well under specified conditions.

The bill establishes other requirements related to completion of the trainings, including (1) granting authority to the SCISO to determine specifications for State employee trainings and granting authority to the chief executives of each local governmental unit to determine specifications for their employees and (2) requiring local governments and chief executives of State agencies to verify to the SCISO that the training is taking place.

Additionally, the Secretary of Information Technology and local governments must conduct periodic audits, as specified, to ensure compliance with these requirements.

Cybersecurity Training Requirements for Contractors

The SCISO must approve a certified training course for contractors whose job duties include accessing a State or local government computer system or database. Each contractor with such access that is awarded a contract by a unit of State or local government must complete an approved training before beginning work under the contract and before any contract renewal term. The contractor must verify completion of the training to the appropriate unit of State or local government, and an employee who oversees a contractor must report the specified related information to the SCISO.

Additionally, a State or local government employee who oversees a contractor must conduct periodic audits to ensure compliance with these requirements.

Current Law:

Protection of Personal Information

Chapter 304 of 2013 requires a unit of State or local government (except for the Legislative and Judicial branches of State government) that collects an individual's personal information to implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. Similarly, a unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices.

"Reasonable security procedures and practices" means data security procedures and practices developed, in good faith, and set forth in a written information security policy. "Personal information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- a Social Security number;
- a driver's license number, State identification card number, or other individual identification number issued by a unit of State government;
- a passport number or other identification number issued by the United States government;
- an individual Taxpayer Identification Number; or
- a financial or other account number, credit card number, or credit card number that (in combination with a security code, access code, or password) would permit access to an individual's account.

Personal information does not include a voter registration number.

Maryland Cybersecurity Coordinating Council

MCCC was created in 2019 by Executive Order 01.01.2019.017 to advise and make recommendations to the SCISO on strategy and implementation of cybersecurity initiatives and recommendations. Further, it provides advice and recommendations for building and sustaining the State's capability to identify, mitigate, and detect cybersecurity risk, as well as how to respond to and recover from cybersecurity-related incidents. MCCC is chaired by the SCISO and includes 11 *ex officio* members, all of which are Secretaries of large or public-safety oriented State agencies.

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

State Fiscal Effect: Since the vast majority of State employees access State computer systems and databases to some extent in their duties (as almost every State employee has a State email address for correspondence), most or all State employees must receive cybersecurity training under the bill. Moreover, DoIT and State agencies must ensure that State contractors receive training as well, if they have access to State systems, which many likely do. DoIT advises that, under its current cybersecurity training practices:

- 60,000 State employees (about 93%) receive annual cybersecurity training;
- this training is provided by one company (Infosec), and the annual cost per user who receives the training is $1.50;
- DoIT contracts with and pays Infosec and collects reimbursable revenues from State agencies; and
- to administer the training program, DoIT uses a third-party contractor for 1.25 full-time-equivalent (FTE) positions at $125 per hour (these costs are borne by DoIT and not the agencies).

Department of Information Technology

The bill's certification, training, and audit requirements are generally split between the Secretary of Information Technology and MCCC. Since MCCC is chaired by the SCISO, who is part of DoIT, for purposes of this analysis, it is assumed that DoIT continues to administer the State's information technology (IT) training program. As noted above, the bill establishes additional requirements and regulatory processes related to cybersecurity training that are substantially different than processes currently in use, and DoIT requires additional staff and resources to handle the new responsibilities. MCCC can develop standards and guidelines for the trainings using existing budgeted resources.

Typically, full-time permanent staff would be most appropriate to perform related duties; however, DoIT advises that it has historically been unable to hire professional staff with the cybersecurity training and expertise required to implement the bill at the salary levels allowed by the State's salary schedule. Therefore, for purposes of this analysis, it is assumed that DoIT engages a third-party contractor to evaluate and certify training programs, work with and audit State agencies, and oversee and administer the cybersecurity training program for State contractors (estimated to be about 90,000 contractors).

Thus, general fund expenditures increase by an estimated $937,500 annually beginning in fiscal 2023. The estimate is based on DoIT's existing contract costs to oversee and administer the cybersecurity program for State employees. Specifically, DoIT pays $125 per hour to its third-party contractor for about 2,500 hours each year (1.25 FTEs) to manage and oversee the provision of cybersecurity training to 60,000 State employees. The estimate includes 3.75 additional FTE staff with cybersecurity expertise from DoIT's current contractor at the same hourly rate and assumes (1) 1.75 additional FTE (totaling $437,500) to provide additional support and oversight for the provision of training to about 90,000 contractors and (2) 2.0 additional FTE (totaling $500,000) to annually evaluate and certify training programs and to perform audits of State agencies and contractors to ensure compliance.

The estimate assumes that the new contract takes effect on July 1, 2023 (fiscal 2024), following the completion of standards in April of that year, so that the contractors can fully organize and develop the necessary processes to begin the auditing and oversight processes when government units begin to meet the bill's training requirements on October 1, 2023.

DoIT advises that expanding its existing training process through Infosec increases total costs across all State agencies by $225,000 annually to train employees not currently receiving training. Since DoIT is a fee-for-service agency, it is assumed that that these costs are passed on to the State agencies. Therefore, reimbursable revenues and expenditures for DoIT increase by $225,000 annually beginning in fiscal 2024, the year that agencies must begin to adhere to the bill's training requirements.

Costs to State Agencies

State agencies are likely to experience additional costs due to the training requirements and processes established by the bill for two reasons.

First, each State agency must administer and oversee cybersecurity training for State contractors. Although additional staff hired by DoIT provide general oversight for this requirement, State agencies likely need to assist in coordinating the trainings and conducting the required audits to ensure compliance. Carrying out these responsibilities

may, in some cases, require additional staffing resources, but a reliable estimate across all agencies is not feasible. Costs associated with those resources are likely to be minimal or nonexistent for many agencies that do not engage many contractors, but they could be significant for larger agencies like the Maryland Department of Transportation.

Second, as contractors receive training, either the State agency will pay for the training directly (resulting in direct additional costs) or require contractors to pay for the training themselves. Contractors may then pass these costs on to State agencies by increasing the price of the contracts. As noted above, DoIT advises that expanding its existing training process through Infosec increases total costs across all State agencies by $225,000 annually. To the extent this is how the bill is implemented, there is no significant impact on any one State agency for the additional training costs.

Local Expenditures: The Maryland Association of Counties advises that all county governments currently require employees to receive some sort of annual cybersecurity training. Based on the responses received for this fiscal and policy note, the training frequency and programs vary from locality to locality. For example, (1) Montgomery County advises that it provides monthly trainings for its employees, but significantly more of its contractors are required to receive training under the bill, increasing costs by about $150,000 annually; (2) Baltimore City advises that it requires employees and contractors to receive quarterly training; and (3) Kent County advises that only its IT staff receive annual cybersecurity training. No local government discussed whether it currently conducts audits to ensure the trainings are taking place.

As such, many local governments are likely to experience additional administrative and contract costs due to the training requirements and processes required by the bill. The total cost could be significant for a local government if its current training program is not certified by MCCC or if it does not currently require any or all contractors to receive cybersecurity training.

Small Business Effect: A small business that provides cybersecurity training and has a program certified by DoIT may experience significantly more business under the bill due to the large of number of State and local employees and contractors who must participate in training.

Additional Information

Prior Introductions: HB 1129 of 2021, a bill with similar provisions, received a hearing in the House Health and Government Operations Committee, but no further action was taken.

Designated Cross File: SB 107 (Senator Jackson) - Education, Health, and Environmental Affairs.

Information Source(s): Department of Information Technology; Department of Commerce; Maryland Department of Aging; Maryland Department of Emergency Management; Office of the Attorney General; Maryland State Treasurer's Office; Judiciary (Administrative Office of the Courts); Maryland State Department of Education; Maryland School for the Deaf; Maryland Higher Education Commission; Maryland State Library Agency; Maryland Department of Agriculture; Maryland Department of the Environment; Department of General Services; Department of Housing and Community Development; Department of Human Services; Department of Juvenile Services; Maryland Department of Labor; Department of Natural Resources; Maryland Department of Planning; Department of Public Safety and Correctional Services; Department of State Police; Maryland Department of Transportation; Department of Veterans Affairs; Health Benefit Exchange; Maryland Insurance Administration; Maryland Association of Counties; Baltimore City; Kent, Montgomery, and Worcester counties; Washington Suburban Sanitary Commission; Maryland Municipal League; Town of Leonardtown; Town of Riverdale Park; Baltimore City Public Schools; Prince George's County Public Schools; Department of Legislative Services

Fiscal Note History: First Reader - January 21, 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.