HB 1129

Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 1129 (Delegate Krimm)
Health and Government Operations

Department of Information Technology – State and Local Government Employees and Contractors – Cybersecurity Training

This bill requires each employee of an Executive Branch agency or a unit of local government, as defined, to annually complete a cybersecurity training program if the employee's job-related duties include accessing government computer systems or databases. The bill also requires the Department of Information Technology (DoIT) in coordination with the Maryland Cybersecurity Council (MCC) to certify the training programs that may be used, requires government contractors to receive cybersecurity training, and establishes related processes that must be followed to meet the bill's requirements. DoIT must adopt regulations to implement the bill.

Fiscal Summary

State Effect: Even though most State employees receive cybersecurity training under current practices, State expenditures (all funds) are likely to increase for training, administrative costs, and additional contract costs, in some cases significantly, as discussed below. General fund expenditures by DoIT increase by $890,600 in FY 2022 and $1.2 million annually thereafter to implement the bill. Reimbursable revenues may offset some of the additional costs to DoIT, as discussed below; this potential revenue is not reflected below.

($ in millions)	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026
Revenues	$0	$0	$0	$0	$0
GF Expenditure	0.9	1.2	1.2	1.2	1.2
GF/SF/FF Exp.	-	-	-	-	-
Net Effect	(-)	(-)	(-)	(-)	(-)

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: DoIT must coordinate with MCC to (1) develop criteria for the certification of cybersecurity training programs for use by State and local government employees; (2) certify at least 20 cybersecurity training programs; (3) annually review and update certification standards for cybersecurity training programs; and (4) maintain on its website a list of all certified programs. The criteria must include specified requirements and DoIT may contract with a third-party to certify the training programs.

At least once each year, each employee of a unit of State or local government must complete a cybersecurity training program that has been certified by DoIT if that employee's job-related duties include accessing government computer systems or databases. A unit is authorized to specify which certified program each employee must complete, as specified, and may set different requirements for different employees. Each unit must report to DoIT each year on the programs that were selected and the percentage of employees that completed each program. DoIT must require periodic audits of units of State government, and local governments must require periodic audits of their units to ensure compliance with the bill.

DoIT must approve at least one certified program to be used to train State and local contractors that have access to a unit's computer systems or databases in safe cybersecurity practices. Each contract entered into by a unit of State or local government must contain a clause requiring each contractor to complete such a program if applicable. Each contractor must complete a program at least once each year during the term of the contract, as specified, and verify the completion to the contracting unit. Each unit of State or local government must report to DoIT each year on which programs each contractor completed and conduct periodic audits to ensure compliance with the bill.

Current Law:

Department of Information Technology

DoIT and the Secretary of Information Technology are responsible for:

- developing and enforcing information technology (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; and
- adopting and enforcing nonvisual access standards to be used in the procurement of IT services, as specified.

The following agencies are exempt from oversight by DoIT:

- public institutions of education for academic or research purposes;
- the Maryland Port Administration;
- the University System of Maryland;
- St. Mary's College of Maryland;
- Morgan State University; and
- the Maryland Stadium Authority.

Maryland Cybersecurity Council

Chapter 358 of 2015 established MCC. The council is required to work with the National Institute of Standards and Technology (NIST), as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State issues. The council's responsibilities include (1) examining inconsistencies between State and federal cybersecurity laws; (2) assisting private-sector cybersecurity businesses in adopting, adapting, and implementing the NIST cybersecurity framework of standards and practices; and (3) recommending legislative changes to address cybersecurity issues.

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

State Expenditures: 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. The Department of Budget and Management advises that about 93% of State employees (about 60,000) already receive annual cybersecurity training from DoIT and the total annual cost for all State agencies related to the training is about $250,000. DoIT

advises that this training is provided by one company (Infosec) and the cost per user who receives the training averages $1.50. Through this process, DoIT contracts with and pays Infosec and collects reimbursable revenues from State agencies.

To implement the bill, DoIT anticipates significant annual contractual costs and many State agencies are likely to experience additional contract and administrative costs because the bill's cybersecurity training requirements and processes are more complex and involved than those currently used by DoIT. DoIT and State agencies must also oversee the training of State contractors. The costs to DoIT and State agencies are discussed below.

Department of Information Technology

As noted above, the bill establishes additional requirements and regulatory processes related to cybersecurity training for DoIT that are substantially different than processes currently in use, and DoIT requires additional staff and resources to handle the new responsibilities. 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 $890,625 in fiscal 2022 (due to the bill's October 1, 2021 effective date) and $1.2 million annually thereafter. 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 full-time-equivalent (FTE)) to manage and oversee the provision of cybersecurity training to 60,000 State employees under DoIT's existing process. The estimate includes 4.75 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) 3.0 additional FTE (totaling $750,000) to annually evaluate and certify training programs and to perform audits of State agencies and contractors to ensure compliance.

DoIT is a fee-for-service agency that generally collects fees from State agencies for most of the services it provides to them. As noted above, this is the service delivery model that DoIT uses to provide cybersecurity training to State agencies under current law. However, the bill requires DoIT to provide services to local governments and to contractors, and it is not clear whether DoIT can collect fees from those entities. Moreover, as DoIT has to

certify at least 20 different training programs, it is not clear if it can establish the same payment arrangements with those training providers that it has with Infosec. For these reasons, general funds are assumed to be used; to the extent that DoIT can collect service fees from State agencies to cover a portion of these expenses, the general fund expenditures are partially offset by reimbursable revenues and/or fees paid by contractors and local governments. However, any such revenues are speculative and are not included in this analysis.

Costs to State Agencies

State agencies are likely to experience additional costs due to the training requirements and processes established by the bill for three 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, the bill adds additional requirements for each agency, including conducting internal audits of contractors to ensure compliance with the training requirements. 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 (MDOT).

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.

Third, the cost per user to receive training may vary considerably under the bill depending on which training programs are certified by DoIT and selected by a State agency. The total impact is likely to be minimal for smaller agencies with fewer staff, and significant for a larger agencies with many staff. For example, MDOT has tens of thousands of staff and contractors that must receive cybersecurity training under the bill. *For illustrative purposes,* the total cost to train 10,000 staff at $1.50 per user is $15,000 and the total cost at $10.00 per user is $100,000.

Local Expenditures: Many local governments, including Anne Arundel, Frederick, and Montgomery counties, and the City of Laurel advise that they already provide cybersecurity training for all their employees. Even so, similar to the effect described above for State agencies, local governments are likely to experience additional administrative and contract costs due to the training requirements and processes established by the bill, especially as they relate to providing and monitoring training by contractors. The total cost could be significant, particularly for a local government that does not currently require its employees or contractors to receive any 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: None.

Designated Cross File: SB 873 (Senator Jackson)(By Request - Joint Cybersecurity, Information Technology, and Biotechnology Committee) - Education, Health, and Environmental Affairs.

Information Source(s): Department of Information Technology; Maryland Department of Transportation; Department of Budget and Management; Maryland Department of Agriculture; Department of Commerce; Department of Natural Resources; Department of General Services; Maryland Department of Health; Maryland Department of Labor; Department of State Police; Maryland Department of Aging; Department of Public Safety and Correctional Services; University System of Maryland; Department of Housing and Community Development; Maryland Association of County Health Officers; Anne Arundel, Baltimore, Charles, Frederick, and Montgomery counties; Baltimore City Public Schools; Baltimore County Public Schools; Prince George's County Public Schools; City of Laurel; Maryland-National Capital Park and Planning Commission; Washington Suburban Sanitary Commission; Department of Legislative Services

Fiscal Note History: First Reader - March 2, 2021
an/mcr

Analysis by: Richard L. Duncan

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

Appendix – Cybersecurity

Cybersecurity Issues

In recent years, cybersecurity and privacy issues have received significant attention from the general public and policymakers as a result of the many ransomware attacks, data breaches, and other cyberattacks that have taken place in the nation and the State. Globally, in 2019 and 2020, the Center for Strategic and International Studies identified over 200 cyberattacks and data breaches (many of which involved the United States) involving (1) government agencies; (2) defense and high tech companies; or (3) economic crimes with losses of more than $1 million. For example, in November 2020, Baltimore County Public Schools' information technology (IT) systems were made unusable by a ransomware attack and the personally identifiable information (PII) of 27.7 million Texas drivers was exposed in a data breach.

In 2019, governments in the State experienced numerous cyberattacks and breaches. Most notably, Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks. Similarly, the Maryland Department of Labor's licensing database was breached, and PII of as many as 78,000 licensees may have been accessed by the hackers.

Recent State Action

In June 2019, the Governor signed Executive Order 01.01.2019.07, which creates the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative creates the Office for Security Management within the Department of Information Technology (DoIT) and charges the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch IT systems. The office is led by the State chief information security officer (SCISO), who is appointed by the Governor. The order also established the Maryland Cybersecurity Coordinating Council to assist SCISO and the office in their duties.

In that same month, DoIT released the State of Maryland Information Technology Security Manual. The manual currently serves as the primary policy for establishing and defining the State's IT security practices and requirements; all State agencies are required to adhere to the manual.

Legislation enacted in 2020 expands and enhances the cybersecurity protocols that govern the collection, processing, sharing, and disposal of PII by public institutions of higher education in the State beginning on October 1, 2024.

Audits of State Agency Cybersecurity Discover PII Vulnerabilities

Over the 2019 interim, the Office of Legislative Audits (OLA) summarized its recent audit findings related to cybersecurity and PII and reported those findings to the Joint Audit and Evaluation Committee in December 2019. OLA found that, from July 2013 through December 2019, approximately 37.9 million PII records existed in State and local government agencies that were not adequately protected with data security controls. Over that same period, 77 of OLA's audits contained findings related to PII. While DoIT and the State have been improving their protection of PII, a 2020 legislative audit found additional issues. For example, in one instance PII was not adequately restricted to employees who should have access to it and instead was visible to over 5,000 State employees.

OLA has previously emphasized the financial cost associated with data breaches by citing the Ponemon Institute, an independent research organization focused on data protection, and IBM, one of the largest computer manufacturers in the world. The two organizations annually publish a report on global data breaches and their economic impacts. The 2020 Cost of a Data Breach Report found:

- the average total cost of a data breach in the United States is $8.6 million; and
- customer PII has the highest cost per record at $150. *For illustrative purposes*, costs for Texas could total $4.2 billion, as a result of the 27.7 million breached records discussed above.

These costs include detection of the breach, escalation, notifications, response, and lost business.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures (NCSL) advises that 38 states, the District of Columbia, and Puerto Rico introduced or considered about 280 bills or resolutions that dealt significantly with cybersecurity in 2020. Some of the key cybersecurity issues considered included:

- requiring government agencies to implement training or specific types of security policies and practices and improving incidence response and preparedness;
- increasing penalties for computer crime or addressing specific crimes, *e.g.*, ransomware;

- regulating cybersecurity within the insurance industry or addressing cybersecurity insurance;
- creating task forces, councils, or commissions to study or advise on cybersecurity issues; and
- supporting programs or incentives for cybersecurity training and education.

Moreover, NCSL reports that 19 states (including Maryland) adopted or enacted significant cybersecurity-related legislation in 2020. Notably, (1) Delaware granted its Department of Technology and Information the authority to develop and implement a comprehensive security program; (2) Georgia is using funds from its Revenue Shortfall Reserve to enhance cybersecurity technologies; (3) Louisiana enacted 10 pieces of legislation to significantly enhance its cybersecurity framework; and (4) Virginia required its chief information officer to develop and annually update a training program for all state employees in security awareness and in procedures for detecting, assessing, reporting, and addressing information security threats.

Notably, in 2019, 31 states adopted or enacted significant cybersecurity-related legislation. Most notably, (1) New York City enacted the Stop Hacks and Improve Electronic Data Security Act, which amended the state's data breach notification law and imposed more expansive data security requirements on companies; (2) Alabama, Delaware, Mississippi, and New Hampshire enacted legislation establishing a comprehensive security framework that insurance companies must implement; and (3) Oregon enacted legislation requiring manufacturers of "connected devices" to equip those devices with reasonable security features.