HB 348

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 348 (Delegate Novotny)
Health and Government Operations

General Assembly and Legislative Branch of State Government - Security Training - Protecting Security-Sensitive Data

This bill requires the General Assembly and each agency or unit of the Legislative Branch to develop, in accordance with Department of Information Technology (DoIT) guidelines, a plan to (1) identify unit personnel who handle security-sensitive data and (2) establish annual security overview training or refresher training for each member and employee who handles security-sensitive data as part of the individual's duties.

Fiscal Summary

State Effect: General fund contractual expenditures for the Department of Legislative Services (DLS) may increase annually beginning in FY 2023, as discussed below. Revenues are not affected. However, the bill potentially conflicts with the separation of powers requirement of the Maryland Constitution, as discussed in the Additional Comments section of this fiscal and policy note.

Local Effect: None.

Small Business Effect: None.

Analysis

Current Law: State law requires each Executive Branch agency or unit to develop, in accordance with guidelines established by the Secretary of Information Technology, a plan to (1) identify unit personnel who handle security-sensitive data and (2) establish annual security overview training or refresher training for each employee who handles security-sensitive data as part of the employee's duties. *Under the bill*, this requirement is

extended to apply to the Maryland General Assembly and any Legislative Branch agency or unit.

"Security-sensitive data" means information that is protected against unwarranted disclosure. The State of Maryland Information Technology Security Manual currently serves as the primary policy for establishing and defining the State's information technology security practices and requirements for Executive Branch agencies.

The Office of Operations and Support Services within DLS is responsible for evaluating and ensuring that appropriate systems are in place to address cybersecurity threats to the work of the General Assembly and DLS.

For additional information on State and national cybersecurity issues, see the **Appendix – Cybersecurity**.

State Expenditures: As noted above, the bill requires the General Assembly and each agency or unit of the Legislative Branch to develop, in accordance with DoIT guidelines, a plan to identify and establish annual training for members and employees who handle security-sensitive data as part of their duties. It is unclear how many individuals are potentially subject to the bill's training requirement; however, for purposes of this fiscal analysis, it is assumed that all members and employees of the General Assembly and all employees of DLS are potentially subject to the bill's requirement, given the privileged nature of various legislative activities and communications. To the extent that contractual assistance is needed in order to develop and conduct the trainings, general fund expenditures for DLS increase beginning in fiscal 2023. Any such costs have not been quantified at this time.

Addition Comments: A letter of opinion provided by the Office of Counsel to the General Assembly for SB 69 of 2021 advised that imposing the Statewide Security Policy for Executive Branch Agencies on the Legislative Branch would likely violate the separation of powers requirement of the Maryland Constitution. Specifically, Article 8 of the Maryland Declaration of Rights states, "[t]hat the Legislative, Executive and Judicial powers of Government ought to be forever separate and distinct from each other; and no person exercising the functions of one of said Departments shall assume or discharge the duties of any other." Further, members of the General Assembly and legislative staff are protected from liability for or inquiry into their legislative activities by an absolute constitutional privilege.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Department of Legislative Services

Fiscal Note History: First Reader - February 18, 2022
fnu2/mcr

Analysis by: Elizabeth J. Allison

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.