HB 879

Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 879 (Delegate R. Watson)
Health and Government Operations Rules

Cybersecurity Coordination and Operations - Maryland Cybersecurity Council Study and Report

This bill requires the Maryland Cybersecurity Council (MCC) to study various issues related to cybersecurity coordination and operations in the State, and develop a comprehensive cybersecurity coordination and response structure and plan for the State based on the findings from the study. MCC must report its findings and recommendations to the Governor and specified committees of the General Assembly by December 1, 2021. **The bill takes effect July 1, 2021, and terminates July 31, 2022.**

Fiscal Summary

State Effect: General fund expenditures by the University System of Maryland (USM) increase by an estimated $50,000 in FY 2022 to complete the required study and develop the required plan. Revenues are not affected.

(in dollars)	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026
Revenues	$0	$0	$0	$0	$0
GF Expenditure	50,000	0	0	0	0
Net Effect	($50,000)	$0	$0	$0	$0

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

Local Effect: The bill does not directly affect local government operations and finances.

Small Business Effect: None.

Analysis

Bill Summary: MCC must study:

- the State's existing cybersecurity programs and coordination policies and efforts, including the responsibilities of the Maryland Emergency Management Agency (MEMA) and Department of Information Technology (DoIT), as well as the coordination of responsibilities between these units;
- cybersecurity coordination and operations programs in other states;
- best practices and recommendations of models for cybersecurity coordination and operations by a state;
- the traits of a government agency or department that is well suited to manage cybersecurity coordination and operations for a state;
- what State agency or department best matches these traits or whether a new State agency or department should be created to manage cybersecurity coordination and operations for the State;
- the needs for cybersecurity coordination and operations by State, local, and nongovernmental entities in the State; and
- issues regarding the constitutional authority of the General Assembly and the Executive Branch to enact and maintain an effective cybersecurity policy for the State.

Current Law:

Maryland Emergency Management Agency

MEMA, which is part of the Military Department, 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. MEMA 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.

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.

Executive Order 01.01.2019.07 established the Office of Security Management within DoIT, managed and supervised by the State chief information security officer. Generally, the office is responsible for the direction, coordination, and implementation of overall cybersecurity strategy and policy for the State. For more information on cybersecurity issues in the State and across the nation, including the executive order, please see the **Appendix – Cybersecurity**.

Maryland Cybersecurity Council

Chapter 358 of 2015 established the Maryland Cybersecurity Council, staffed by the University of Maryland University College (now called the University of Maryland Global Campus, which is part of USM). 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.

State Expenditures: Due to the amount of information that must be collected to inform the study and plan required by the bill, MCC is likely to need temporary contractual assistance to conduct the study and develop the recommendations by December 1, 2021. Thus, general fund expenditures increase by an estimated $50,000 in fiscal 2022 only for USM to engage temporary contractual assistance to help research and conduct the required study and develop the recommendations.

Additional Information

Prior Introductions: None.

Designated Cross File: SB 69 (Senators Hester and Simonaire) - Education, Health, and Environmental Affairs.

Information Source(s): Department of Information Technology; Office of the Attorney General; University System of Maryland; Montgomery and Worcester counties; Maryland Association of Counties; City of Salisbury; Maryland Municipal League; towns of Bel Air and Leonardtown; Department of State Police; Military Department; Department of Legislative Services

Fiscal Note History: First Reader - February 8, 2021
rh/mcr Third Reader - April 12, 2021
Revised - Amendment(s) - April 12, 2021

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.