HB 1618

Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 1618 (Delegate M. Jackson)
Rules and Executive Nominations

Maryland Emergency Management Agency – Cybersecurity Coordination and Operations Office – Establishment

This bill establishes the Cybersecurity Coordination and Operations Office within the Maryland Emergency Management Agency (MEMA). The bill establishes various responsibilities for the office that generally relate to improving cybersecurity readiness and response in the State. The bill also expands the definition of "emergency," as it relates to provisions governing MEMA, to include a cybersecurity attack. Accordingly, provisions of the Maryland Emergency Management Agency Act that relate to emergencies explicitly apply to cybersecurity attacks.

Fiscal Summary

State Effect: General fund expenditures increase by $369,600 in FY 2021; future year expenditures are annualized and reflect ongoing costs. Revenues are not affected.

(in dollars)	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
Revenues	$0	$0	$0	$0	$0
GF Expenditure	369,600	444,200	454,800	469,700	485,200
Net Effect	($369,600)	($444,200)	($454,800)	($469,700)	($485,200)

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

Local Effect: The bill is not anticipated to directly affect local finances; however, local jurisdictions benefit from support services, assistance, and coordination provided by the office.

Small Business Effect: None. The bill does not directly affect small businesses.

Analysis

Bill Summary: The stated purpose of the Cybersecurity Coordination and Operations Office is to:

- improve local, regional, and statewide cybersecurity readiness and response;
- assist political subdivisions, school boards, and agencies in the development of cybersecurity disruption plans;
- in consultation with the Department of Information Technology (DoIT), coordinate with political subdivisions, local agencies, and State agencies on the implementation of cybersecurity best practices;
- coordinate with political subdivisions and agencies on the implementation of DoIT's Statewide Master Plan; and
- consult with the State Chief Information Security Officer (SCISO) and the Secretary of Information Technology to connect political subdivisions and agencies to the appropriate resources for any other purpose related to cybersecurity readiness and response.

The head of the office is the executive director, who is appointed by the Director of MEMA. The office must be provided with sufficient staff to perform its functions.

The office must establish regional assistance groups to deliver or coordinate support services to political subdivisions, agencies, or "regions." The bill defines "region" as a collection of political subdivisions.

To deliver or coordinate those services, the office may hire or procure regional coordinators. The office must provide or coordinate support services that include (1) connecting multiple political subdivisions and agencies with each other to share best practices or other information to increase readiness or response effectiveness; (2) providing technical services for the implementation of cybersecurity best practices; (3) completing cybersecurity risk assessments; (4) developing cyberscorecards and reports on regional readiness; (5) creating and updating cyber disruption plans; and (6) conducting regional exercises in coordination with the National Guard, MEMA, DoIT, local emergency managers, and other State and local entities.

The office must report to the Governor and the General Assembly by December 1 of each year on its activities.

Current Law/Background:

Maryland Emergency Management Agency and Gubernatorial Powers

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.

The Governor has control of and is responsible for MEMA and is responsible for carrying out the provisions of the Maryland Emergency Management Agency Act. In the event of the threat or occurrence of an emergency, the Governor may assume direct operational control over all or part of an emergency management function created or authorized by the Act. The Act enumerates specific powers the Governor has relating to emergency management. Among other things, if the Governor finds that an emergency has developed or is impending due to any cause, the Governor must declare a state of emergency by executive order or proclamation.

Cybersecurity Issues

In recent years, technological advancements to networks, electronic devices, and other forms of information technology have expanded and improved communications, travel, and data analysis. The U.S. Department of Homeland Security reports that cyber intrusions and attacks have also increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing steep economic costs.

Executive Order 01.01.2019.07 established the Office of Security Management within DoIT, managed and supervised by the SCISO. 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.**

Department of Information Technology's Statewide Master Plan

The Statewide Master Plan, produced by DoIT, is a guide to assist State agencies in selecting technology services to support existing operations, in addition to acting as a roadmap for fostering innovation and services that government provides. Among other things, the plan details how DoIT attempts to reduce cybersecurity risks across all State

agencies, such as establishing weekly vulnerability reviews and monthly cybersecurity situational awareness reporting.

Maryland Cybersecurity Council

Chapter 358 of 2015 established the Maryland Cybersecurity Council. 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. In the council's 2016 interim report and 2017 report, numerous recommendations were made to improve the cybersecurity of the State's critical infrastructure.

State Expenditures: General fund expenditures for MEMA increase by $369,630 in fiscal 2021, which accounts for the bill's October 1, 2020 effective date. This estimate reflects the cost of hiring one executive director to lead the office and provide strategic and programmatic oversight, two regional coordinators to work with DoIT and provide assistance to State agencies and local jurisdictions, and one administrator to provide overall administrative support. It includes salaries, fringe benefits, one-time start-up costs (including the purchase of laptops), and ongoing operating expenses, including travel and office rent. As MEMA does not have enough office space to house the new office, the department must rent additional office space. In addition, it is assumed that staff regularly travel to State agencies and local jurisdictions in order to implement the bill's various requirements.

Positions	4.0
Salaries and Fringe Benefits	$329,165
Operating Expenses	40,465
Total FY 2021 State Expenditures	**$369,630**

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

DoIT advises that it can coordinate and consult with the office and affected State and local agencies using existing resources. The bill is not anticipated to have a direct effect on the finances of other State agencies; however, other agencies benefit to the extent the office provides cybersecurity services or assistance that otherwise would not be readily available.

Additional Information

Prior Introductions: None.

Designated Cross File: SB 1036 (Senator Hester) - Education, Health, and Environmental Affairs.

Information Source(s): Department of Information Technology; Maryland Association of Counties; Maryland Municipal League; Department of State Police; Military Department; Department of Legislative Services

Fiscal Note History: First Reader - April 17, 2020
rh/lgc

Analysis by: Thomas S. Elder

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 cyber attacks that have taken place in the nation and the State. Globally, and in 2019 alone, the Center for Strategic & International Studies (CSIS) identified nearly 100 known cyber attacks (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.

Also in 2019, governments in the State experienced numerous cyber attacks and breaches. Most notably, Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible to government officials and employees. The systems remained unavailable for weeks, and recovery is still ongoing. Similarly, the Maryland Department of Labor's licensing database was breached, and the personally identifiable information (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 information technology (IT) systems. The office is led by a newly created 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 office in its 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.

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.

OLA also 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 2019 Cost of a Data Breach Report found:

- during an average data breach, 25,575 records are accessed;
- the average total cost of a data breach is $8.2 million; and
- the average cost per lost record is $242.

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

Cybersecurity Legislation in Other States

The National Conference of State Legislatures advises that 43 states and Puerto Rico introduced or considered about 300 bills or resolutions that dealt significantly with cybersecurity in 2019. Some of the key cybersecurity issues considered included:

- appropriating funds for improved security in government;
- addressing cybersecurity threats to elections;
- requiring government agencies to implement training and security policies and practices;
- creating cybersecurity task forces, commissions, or studies;
- targeting cyber threats such as ransomware or other computer crimes;
- addressing cybersecurity within the insurance industry or cybersecurity insurance for government;
- providing for the confidentiality of government cybersecurity information and plans by exempting it from public records laws;
- encouraging cybersecurity training, education, and workforce development;
- studying the use of blockchain for cybersecurity;

- requiring the private sector to improve security practices; and
- addressing the security of connected devices.

Moreover, 31 states adopted or enacted significant cybersecurity-related legislation in 2019. 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 passed 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.