HB 898

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 898 (Delegate Rosenberg)
Appropriations

Maryland Department of Emergency Management - Office of Domestic Terrorism Response

This bill establishes the Office of Domestic Terrorism Response in the Maryland Department of Emergency Management (MDEM). The purpose of the office is to develop strategies and resources to prepare for, prevent, and recover from domestic terrorism activities. By December 1 each year, MDEM must report to the Governor and the General Assembly on the activities of the office.

Fiscal Summary

State Effect: General fund expenditures increase by $253,800 in FY 2023; future years are annualized, adjusted for inflation, and reflect ongoing costs. State revenues are not directly affected but could be indirectly affected to the extent the establishment of the office enables the State to secure additional federal grants (not reflected below).

(in dollars)	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
Revenues	$0	$0	$0	$0	$0
GF Expenditure	253,800	304,200	312,700	321,000	329,400
Net Effect	($253,800)	($304,200)	($312,700)	($321,000)	($329,400)

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

Local Effect: The bill is not anticipated to have a direct effect on local operations or finances.

Small Business Effect: None.

Analysis

Bill Summary: The office must (1) coordinate with federal, State, and local agencies in developing and implementing plans related to domestic terrorism prevention and response, including cybersecurity attacks; (2) consult with the academic community to identify trends and develop best practices for the prevention of domestic terrorism; (3) explore federal grant funding opportunities; (4) engage with public health professionals to discover and implement early intervention strategies in persons becoming radicalized or at risk of committing an act of terrorism; (5) coordinate with federal law enforcement to explore methods to encourage and facilitate early reporting of emerging terrorism threats; and (6) research strategies employed by other states to prevent and respond to domestic terrorism threats.

Current Law:

Domestic Terrorism – Generally

Under federal law (18 U.S.C. § 2331), domestic terrorism means activities that (1) occur primarily within the territorial jurisdiction of the United States; (2) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any state; and (3) appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnapping.

Maryland Department of Emergency Management

Chapters 287 and 288 of 2021 established MDEM as a principal department of the Executive Branch of State government and as the successor to the Maryland Emergency Management Agency. MDEM 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 (FEMA) and other federal partners. MDEM 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 *2021 Joint Chairmen's Report* required MDEM to convene a Task Force on Preventing and Countering Domestic Terrorism to determine how to effectively oppose domestic terrorism in the State. Among other responsibilities, the task force was required to detail how Homeland Security Grant Program funds (federally administered by FEMA, distributed by MDEM) should be expended. In addition, the task force was required to detail how the program funds received by MDEM have been expended to support programs

to counter domestic terrorism. MDEM submitted its findings to the Senate Budget and Taxation Committee and the House Appropriations Committee on November 15, 2021.

Governor's Office of Homeland Security

Established by regulation, the Governor's Office of Homeland Security is responsible for directing homeland security efforts across State government and coordinates with federal and local governments, the private sector, academia, and the public to find solutions that ensure public safety while protecting individual freedoms. Among other things, the director of the office is responsible for advising the Governor on policies, strategies, and measures to enhance and improve the ability to detect, prevent, prepare for, protect against, respond to, and recover from man-made emergencies or disasters, including terrorist attacks. The director is also generally responsible for coordinating homeland security activities within the State and coordinating with federal and local governments. The office has three staff positions, including one deputy director who shares office space at MDEM.

Fusion Centers and the Maryland Coordination and Analysis Center

Fusion centers are a collaborative effort of two or more federal, State, or local government agencies that combine resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity. Generally, fusion centers receive information and intelligence from a variety of sources and disseminate the information to all levels of government to identify and address immediate and emerging threats.

The Maryland Coordination and Analysis Center (MCAC) is the State's only fusion center and is housed in the Department of State Police. Among other responsibilities, MCAC collects and distributes domestic terrorism intelligence and analysis to federal, State, and local stakeholders and law enforcement agencies.

Cyberattacks and Cybersecurity in the State

For information on recent cyberattacks affecting State agency and local government information systems and recent legislation and gubernatorial action taken to address cybersecurity and information technology issues in the State, please see the **Appendix – Cybersecurity.**

State Expenditures: General fund expenditures increase by $253,777 in fiscal 2023, which accounts for the bill's October 1, 2022 effective date. This estimate reflects the cost of hiring (1) one domestic terrorism unit leader to oversee the office and develop strategies to prepare for, prevent, and recover from domestic terrorism, in addition to seeking federal grant funding opportunities; (2) one planning specialist to coordinate with federal, State,

and local agencies in developing and implementing plans related to domestic terrorism; and (3) one analyst to coordinate with the academic community, develop best practices for preventing domestic terrorism, engage with public health professionals regarding early intervention strategies, and conduct research on strategies employed by other states. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	3.0
Salaries and Fringe Benefits	$231,748
Operating Expenses	22,029
Total FY 2023 State Expenditures	**$253,777**

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

MDEM advises that the department requires additional contractual support, estimated at $175,000 annually, to develop the required annual report and to consult with subject matter experts in order to meet the bill's requirements. The Department of Legislative Services disagrees, as it is expected that the staff of the office can develop the report and be subject matter experts to fulfill the bill's requirements. Should the estimated staff prove insufficient, MDEM can request additional resources through the annual budget process.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Baltimore, Garrett, and Montgomery counties; Maryland Department of Emergency Management; City of Laurel; Maryland Municipal League; University System of Maryland; Morgan State University; Maryland Department of the Environment; Maryland Department of Health; Department of State Police; Maryland Department of Transportation; Public Service Commission; U.S. Department of Homeland Security; Department of Legislative Services

Fiscal Note History: First Reader - March 8, 2022
fnu2/mcr

Analysis by: Thomas S. Elder

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.