Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 5 (Senator Hester)
Education, Health, and Environmental Affairs

Public Safety - Maryland Cyber Reserve - Established

The bill establishes the Maryland Cyber Reserve (MCR) within the Military Department. The primary mission of MCR is to provide educational and technical support to prevent and resolve cyber attacks against State, county, and local government agencies and associated critical infrastructure.

Fiscal Summary

State Effect: General fund expenditures increase by *at least* $29,000 in FY 2021 and by *at least* $38,700 annually, which only reflects costs to acquire workers' compensation insurance and office space, as discussed below. Revenues are not affected.

(in dollars)	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
Revenues	$0	$0	$0	$0	$0
GF Expenditure	29,000	38,700	38,700	38,700	38,700
Net Effect	($29,000)	($38,700)	($38,700)	($38,700)	($38,700)

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

Chesapeake Employers' Insurance Company (Chesapeake) Effect: Chesapeake nonbudgeted revenues increase by $8,400 in FY 2021 and by $11,200 annually thereafter from workers' compensation premiums. Chesapeake nonbudgeted expenditures increase minimally to the extent that additional workers' compensation claims are paid.

(in dollars)	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
NonBud Rev.	$8,400	$11,200	$11,200	$11,200	$11,200
NonBud Exp.	-	-	-	-	-
Net Effect	-	-	-	-	-

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

Local Effect: The bill is not anticipated to materially affect local finances or operations.

Small Business Effect: None.

Analysis

Bill Summary:

Establishment of the Maryland Cyber Reserve within the Military Department

MCR is a component of the organized militia of the State in addition to and separate from the National Guard. The Governor is the commander-in-chief of MCR, and MCR is under the operational control of the Adjutant General. There is a commanding general of MCR who is appointed by the Adjutant General and serves at his/her pleasure.

In addition to its primary mission, MCR must also have other duties and missions, including providing technical support to (1) corporations conducting business within the State targeted in a cyber attack and (2) citizens of the State targeted in a cyber attack.

Regulations

The Governor is authorized to adopt regulations to implement the bill's provisions governing the enlistment, organization, administration, equipment, maintenance, training, and discipline of MCR. The Governor may prescribe a uniform for MCR. The regulations must prohibit MCR or a member of MCR from accepting gifts, donations, gratuities, or anything of value from a person in exchange for specific and isolated services rendered by MCR. However, this may not be interpreted to prohibit gifts, bequests, and the like from any individual or organization to MCR or any foundation or the like established to support its activities.

Composition

MCR consists of (1) commissioned or assigned officers and (2) qualified individuals who volunteer to serve and are commissioned, appointed, or enlisted in MCR. An individual may not be commissioned or enlisted in MCR if he/she (1) is not a citizen of the United States; (2) has been dismissed from or received a specified discharge from a military or naval organization of the State or of another state or has been convicted of a federal or state offense, as specified; or (3) does not meet the qualifications for commissioning, appointment, or enlistment specified in regulations governing MCR. Specified clubs and civic organizations may not enlist in MCR as an organization or unit.

Compensation

All members of MCR serve on a voluntary basis and without pay, unless under orders, approved by the Adjutant General, specifying that the member's service is with pay. If an order approved by the Adjutant General specifies that the service of a member of MCR is

with pay, the member must receive a rate of pay determined and provided by rule by the Adjutant General. The rule must establish a rate of pay reasonable and commensurate with the training, experience, and professional qualifications of the member.

Enlistment and Resignations

An officer or warrant officer commissioned or appointed in MCR must take a specified oath. The enlistment period in MCR is determined by the commanding officer based on the specialty of the recruit and the needs of the militia and may be renewed. In the case that a state of war exists between the United States and any other nation, or that there is a federal or State declaration of emergency presently in force in the State, all enlistments must continue three months after said state of war or emergency ends, unless the enlisted individual is discharged sooner by proper authority. The Governor may accept the resignation of an officer or grant a discharge to an enlisted individual at any time.

Requisitions by the Governor

The Governor may requisition any arms and equipment from the U.S. Secretary of Defense that are in the possession of and can be spared by the U.S. Department of Defense (DOD) for use by MCR. The Governor may allow MCR to use the facilities and equipment of a State armory or other available State premises and property. A school authority is authorized to allow MCR to use a school building or school grounds.

Federal Service

MCR may not be ordered or drafted into the military service of the United States, except by order of the President of the United States acting pursuant to the U.S. Constitution and federal law. However, this may not be construed to prohibit service of MCR or personnel in missions in which federal military personnel are also serving or in command. An individual is not exempt from military service under federal law because the individual is enlisted, commissioned, or appointed in MCR.

Appointment and Commissioning of MCR Officers

The Governor must appoint and commission each commissioned officer or appoint each warrant officer of the organized militia on recommendation of the Adjutant General. The appointments do not require confirmation by the Senate of Maryland.

Each individual commissioned or appointed as an officer or warrant officer must be (1) an officer, a warrant officer, or an enlisted individual of the National Guard; (2) a retired or former officer or warrant officer of, or an individual with prior enlisted service in, the U.S. Army, Navy, Marine Corps, Air Force, or Coast Guard (or any auxiliary thereof); (3) a

graduate of the U.S. Military Academy, Naval Academy, Coast Guard Academy, Merchant Marine Academy, or Air Force Academy; (4) a graduate of specified schools who received military instruction under the supervision of specified U.S. military officers who certified the graduate's fitness for appointment as a commissioned officer; or (5) an individual not otherwise identified in items (1) to (4) who is specially qualified for service by achievement in any professional, technical, or public service capacity or otherwise displays extraordinary qualifications for commissioning as an officer of MCR. Before taking office, a specified oath must be taken.

When initially appointed, a general officer or colonel of the organized militia must (1) be an officer in the National Guard of a grade of O-4 or higher or (2) have served in any component or auxiliary of the U.S. Army, Navy, Marine Corps, Air Force, or Coast Guard or National Guard with the grade of O-4 or higher. In addition, when initially appointed, a lieutenant colonel or major of the line must have had service as an officer for at least two years in any component or auxiliary of the U.S. Army, Navy, Marine Corps, Air Force, or Coast Guard or National Guard. However, these requirements do not apply in the case of officers promoted to the grade of major or above from within MCR or specified other officers.

Workers' Compensation

The Adjutant General must secure workers' compensation insurance with Chesapeake for each officer and enlisted individual of MCR. This provision applies when an employee is ordered by the Governor to active military duty for service during a cyber attack. In addition, the Adjutant General must maintain workers' compensation insurance for members of MCR during training. The Adjutant General must pay the premiums for the insurance policy from appropriations for the militia that the Governor includes in the State budget.

Current Law/Background:

Adjutant General, Maryland Defense Force, and State Cyber Units

The Adjutant General heads the Military Department, is responsible for the department's budget, and is custodian of all State and federal property used by the organized militia. The Adjutant General maintains all State-owned armories located in Maryland and all other properties that may be occupied, purchased, or leased by the Military Department. The Adjutant General also regulates the use of such facilities.

The Maryland Defense Force (MDDF) was formally established by the General Assembly in 1917 and is a uniformed military agency of volunteers under the Adjutant General and the Military Department. MDDF has the primary mission of providing competent

supplemental professional, technical, and military support to the Maryland Army National Guard, the Maryland Air National Guard, and the Maryland Emergency Management Agency. The Governor is the commander-in-chief of MDDF, and MDDF generally cannot be deployed outside the borders of Maryland. State active duty may be required for imminent public crises (such as disasters, rioting, catastrophes, and other general periods of unrest), when martial law is declared, to enforce the laws, or to carry on any function of the State militia.

Within MDDF, the Cyber Security Unit (CYSEC) provides professional, civilian-military expertise in cyber security to the Military Department and State and local agencies as a service and assistance to their own cyber security programs. As of November 2019, there were 12 members of CYSEC.

The 169th Cyber Protection Team of the Maryland Army National Guard is a team of cyber professionals whose mission is to defend DOD information networks and assist in cyber defense issues. As of November 2019, there were 39 full-time soldiers assigned to this unit.

The 175th Cyberspace Operations Group of the Maryland Air National Guard are tasked with cyber offense and defense activities while supporting the U.S. Cyber Command. As of November 2019, there were approximately 300 airmen assigned to this unit.

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.

The first recommendation from the Maryland Cybersecurity Council's 2016 interim report was the creation of a "cyber first responder reserve." That recommendation was repeated in the council's 2017 report.

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.

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

Maryland Workers' Compensation Act

All employers in Maryland are required to provide workers' compensation coverage for their employees. The cost to the employer varies by industry, and there are approximately 600 industrial classifications. To maintain coverage, most employers' must purchase workers' compensation insurance. However, the State (and some local governments) are self-insured, meaning they pay claims directly when and if they happen.

For compensable injuries and occupational diseases, workers' compensation benefits include wage replacement, medical treatment, death and funeral costs, and vocational rehabilitation expenses. The medical care and treatment must be provided for an appropriate time period, depending on the nature and type of personal injury, compensable hernia, or occupational disease. Wage replacement benefits are based on the employee's average weekly wage and on the type of injury, as prescribed in statute; however, in all cases, an employee's weekly benefits may not exceed a certain percentage of the State average weekly wage.

State Expenditures: The Military Department advises that in order to meet the bill's requirements, it requires 11 new volunteers that are not currently serving in other capacities within MDDF; the stated mission of MCR exceeds the currently assigned mission of CYSEC, the department's existing cybersecurity unit. Therefore, a new unit is required. As the Military Department does not have enough office space to house the new unit, it must rent additional office space. In addition, the department advises that the annual premium for workers' compensation insurance is $1,016 per individual insured. Therefore, general fund expenditures increase by *at least* $29,007 in fiscal 2021, which accounts for the bill's October 1, 2020 effective date, and by *at least* $38,676 in fiscal 2022 and annually thereafter. This estimate reflects the cost for the Military Department to (1) provide workers' compensation insurance for 11 MCR members and (2) rent office space for the MCR headquarters. This estimate assumes that the Military Department maintains workers' compensation insurance for MCR members at all times. The estimated costs for insurance and rent are higher to the extent there are more than 11 MCR members.

The Military Department further advises that MCR members are only *paid* if activated by the Governor and if the Adjutant General specifies that a member's service is with pay, provided by rule by the Adjutant General. In such a case, as provided by the bill, a member's pay is generally based on his/her experience and qualifications. In contrast, the

Military Department advises that MDDF members' pay when activated is generally based on the pay given to similarly ranked Maryland National Guardsmen. *For illustrative purposes only*, based on actual pay for Maryland National Guardsmen, general fund expenditures for compensation to MCR members could increase by approximately $42,000 if all 11 MCR members are activated for a period of 30 days, not accounting for basic allowances for subsistence and housing; costs may be higher, however, since the bill requires that the pay rate for MCR members must be commensurate with the training, experience, and professional qualification of the members.

This estimate does not include hardware, software, and other relevant cybersecurity equipment costs that are likely incurred by MCR; systems used for national security purposes are generally classified. The estimate also does not include any additional costs for other equipment or supplies for MCR members, such as uniforms.

Finally, the estimate assumes that MCR is a *reactive* force and is activated only in the event of a cyber attack. The Department of Legislative Services notes, however, that the primary mission of MCR relates also to *preventing* cyber attacks. To the extent MCR is expected to conduct ongoing activities, additional MCR volunteers are needed, resulting in additional costs.

Chesapeake Effect: Chesapeake nonbudgeted revenues increase by $8,382 in fiscal 2021 (due to the bill's October 1, 2020 effective date) and by $11,176 annually thereafter as it collects premiums for workers' compensation insurance policies purchased for MCR members**.** Chesapeake advises that claims for Military Department members vary significantly, but that claims are rare. Therefore, any resulting expenditures are anticipated to be minimal.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Department of Budget and Management; Governor's Office; Military Department; Chesapeake Employers' Insurance Company; Baltimore City Public Schools; Baltimore County Public Schools; Prince George's County Public Schools; Cisco Systems; Department of Legislative Services

Fiscal Note History: First Reader - March 9, 2020
an/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.