HB 1339

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 1339 (Delegate Kerr)
Economic Matters

Cybersecurity - Critical Infrastructure and Public Service Companies (Critical Infrastructure Security Act of 2022)

This bill establishes a Critical Infrastructure Cybersecurity Grant Program in the Maryland Department of Emergency Management (MDEM) to leverage funds available to make cybersecurity improvements to critical infrastructure. It also adds various requirements related to critical infrastructure cybersecurity for (1) MDEM; (2) the Public Service Commission (PSC); (3) the Office of People's Counsel (OPC); and (4) public service companies operating in the State. **The bill takes effect June 1, 2022.**

Fiscal Summary

State Effect: No effect in FY 2022. General fund expenditures may increase in FY 2023, potentially significantly, to fund the grant program, as discussed below; this potential funding is not shown below. General fund administrative expenditures for MDEM increase by $475,000 in FY 2023; future years reflect ongoing costs. Special fund expenditures for PSC increase by $307,200 in FY 2023; future years reflect ongoing costs. Special fund revenues for PSC increase correspondingly from assessments imposed on public service companies. OPC can likely implement the bill using existing budgeted resources.

(in dollars)	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026
SF Revenue	$0	$307,200	$298,900	$307,000	$314,900
GF Expenditure	$0	$475,000	$455,100	$468,100	$480,500
SF Expenditure	$0	$307,200	$298,900	$307,000	$314,900
Net Effect	$0	($475,000)	($455,100)	($468,100)	($480,500)

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

Local Effect: Local finances are likely affected beginning in FY 2023, as discussed below.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary:

Definitions

"Critical infrastructure" means systems and assets, whether physical or virtual, that are so vital to the State that the incapacity or destruction of the system or asset would have a debilitating impact on any one or combination of (1) security; (2) economic security; (3) public health; or (4) public safety. "Security by design" means the consideration of cybersecurity risk in every phase of a project.

"Cyber resiliency" means the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by a cyber resource. "Cyber resource" means an information system that creates, stores, processes, manages, transmits, or disposes of information in an electronic format and can be accessed by a network or by using networking methods.

"Zero trust" means a cybersecurity approach focused on cybersecurity resource protection and based on the premise that trust is never granted implicitly but must be continually evaluated.

Maryland Department of Emergency Management – Grant Program

MDEM is authorized to reduce the disaster risk and vulnerability of critical infrastructure in the State. MDEM must administer the Critical Infrastructure Cybersecurity Grant Program, establish application procedures for the program, and award grants from the program.

In determining the types of cybersecurity improvements and recipients eligible for grants through the program, MDEM must (1) consult with electric companies, gas companies, water utilities, State agencies, and political subdivisions to identify cybersecurity risks and prepare a report on those risks; (2) identify funding to fund the grants awarded under the program; and (3) develop criteria for selecting grant recipients, as specified. The report must be submitted to the Governor and the General Assembly by December 1, 2022.

MDEM must require each grant recipient to develop processes to address cybersecurity risks and submit a report on implemented processes, as specified. MDEM must also require grant recipients that modernize or improve the resilience of electric grids, natural gas infrastructure, or water and sewer systems to submit a report on implemented security by design principles to MDEM and establish a cybersecurity plan that addresses cybersecurity risks in policy, software development, hardware, and networks.

Public Service Commission and Public Service Companies

PSC must include on its staff one or more employees dedicated to cybersecurity policy, strategy, auditing, and reporting. In supervising and regulating public service companies, PSC must consider the cybersecurity risks faced by public service companies in the State. By June 31, 2023, PSC must update its existing regulations that implement service quality and reliability standards relating to the delivery of electricity to retail customers, as specified, by including standards related to cyber resiliency.

Except for a public service company that is a common carrier or a telephone company, each public service company must:

- adopt cybersecurity best practices, including implementing zero trust principles;
- protect personally identifiable information (PII) of customers and employees;
- include in contracts with third-party information technology or operational technology providers provisions requiring the third-party providers to (1) collect and preserve data for cybersecurity analysis and (2) share that data and report any cybersecurity breaches to the public service company;
- establish minimum security standards for information technology and operational technology devices; and
- encrypt and create minimum security standards for data and PII held by the public service company.

Office of People's Counsel

OPC may hire or retain as necessary experts in the field of cybersecurity.

Current Law:

Public Service Commission and Office of People's Counsel

PSC must supervise and regulate public service companies subject to its jurisdiction to (1) ensure their operation in the interest of the public and (2) promote adequate, economical, and efficient delivery of utility services in the State without unjust discrimination. In doing so, PSC must consider the public safety, the economy of the State, the maintenance of fair and stable labor standards for affected workers, the conservation of natural resources, the preservation of environmental quality, and the achievement of the State's climate commitments for reducing statewide greenhouse gas emissions. PSC must also enforce compliance with legal requirements by public service companies.

Broadly, OPC represents the interests of residential and noncommercial users of natural gas, electricity, telephone, and private water service before PSC, various federal regulatory commissions, and the courts. Specific authorities and requirements include:

- OPC must evaluate each matter pending before PSC to determine if the interests of residential and noncommercial users are affected, and if OPC determines that to be so, OPC must appear before PSC and courts on behalf of the State and its residents in each matter or proceeding over which PSC has original jurisdiction;
- OPC may retain or hire experts in relevant fields;
- as OPC considers necessary, OPC must conduct investigations and request PSC to initiate proceedings to protect the interests of residential and noncommercial users; and
- OPC is entitled to the assistance of PSC staff if the staff determines that the assistance is consistent with the staff's responsibilities and if the staff and OPC agree that the assistance, in a particular matter, is consistent with their respective interests.

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 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. Each local government has a Local Emergency Management Director who works with MDEM on behalf of the local government during a major emergency or disaster.

Cybersecurity

For information on recent cyber-attacks 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 Fiscal Effect:

Maryland Department of Emergency Management

The purpose of the Critical Infrastructure Cybersecurity Grant Program established by the bill is to leverage funds available from federal, State, and local grant programs to make cybersecurity improvements to critical infrastructure. The Department of Legislative Services is unaware of any such State or local level grant programs; however, there may be federal grant program funding available. Absent any other funding source, significant general funds (likely in excess of $1.0 million annually) are likely necessary beginning in fiscal 2023 to ensure a viable and effective program. This estimate does not include any potential funding for the grant program; however, to the extent State, local, or federal funding becomes available, revenues and expenditures increase accordingly.

MDEM does not currently have direct responsibilities related to or staff with specific expertise in disaster risk reduction for critical infrastructure, and it also requires additional staff to administer the grant program. Therefore, general fund expenditures by MDEM increase by $474,959 in fiscal 2023, which assumes a 30-day start-up delay from the bill's June 1, 2022 effective date. This estimate reflects the cost of hiring five full-time staff and one half-time staff, including a critical infrastructure risk reduction specialist, a program manager and program administrator, a grant specialist, a fiscal services officer, and a half-time human resources officer. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	5.5
Salaries and Fringe Benefits	$429,812
Operating Expenses	45,147
Total FY 2023 MDEM Expenditures	**$474,959**

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

Public Service Commission

Special fund expenditures for PSC increase by $307,177 in fiscal 2023, which assumes a 30-day start-up delay from the bill's June 1, 2022 effective date. This estimate reflects the cost of hiring three full-time information technology and cybersecurity expert staff to handle policy and strategy development, auditing and other enforcement activities, and reporting, as required by the bill. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

Positions	3.0
Salaries and Fringe Benefits	$276,087
Operating Expenses	31,090
Total FY 2023 PSC Expenditures	**$307,177**

Future year expenditures reflect annual increases and employee turnover as well as annual increases in ongoing operating expenses. Special fund revenues increase correspondingly from assessments imposed on public service companies, as authorized under current law.

Office of People's Counsel

OPC advises that it can likely handle the bill's additional responsibilities using existing budgeted resources.

Local Fiscal Effect: Numerous local government entities throughout the State, such as municipal electric and water utilities, are likely subject to the cybersecurity requirements established by the bill. Depending on the current practices and disposition of these entities, local government expenditures may increase, potentially significantly, to comply with the bill.

Local governments are also likely eligible to apply to the Critical Infrastructure Cybersecurity Grant Program for grants to make cybersecurity improvements to critical infrastructure. To the extent they receive grants under the program, local grant revenues and expenditures increase correspondingly.

Small Business Effect: To the extent any public service companies – such as private water or sewage disposal companies – are considered small businesses, they may also incur costs to comply with the bill. Small businesses may also be eligible to apply for grants to make cybersecurity improvements to critical infrastructure.

Additional Information

Prior Introductions: None.

Designated Cross File: SB 810 (Senator Hester) - Finance.

Information Source(s): Maryland Department of Emergency Management; Office of People's Counsel; Public Service Commission; Department of Information Technology; Department of Legislative Services

Fiscal Note History: First Reader - March 2, 2022
js/mcr

Analysis by: Richard L. Duncan

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.