Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 390 (The President, *et al.*) (By Request - Administration)
Education, Health, and Environmental Affairs

State Government - Information Technology - Cybersecurity

This Administration bill codifies Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative, and grants the Office of Security Management (OSM) express authority to defend the State's information systems and respond to cyber-attacks against the State-operated telecommunication and computer network. By April 1, 2023, each agency and unit of the Executive Branch of State government must report to the Governor on the information technology (IT) systems it uses, data it stores, cloud or statistical analysis system solutions it uses, and vendor interconnections that are in place. Additionally, by December 1 of each year, each unit of the Legislative and Judicial branches of State government that uses the State-operated local access transport area (LATA) broadband network must certify to the Department of Information Technology (DoIT) that it is in compliance with DoIT's minimum cybersecurity standards.

Fiscal Summary

State Effect: The bill is not anticipated to materially affect State operations or finances, as discussed below.

Local Effect: The bill does not directly affect local governmental operations or finances.

Small Business Effect: The Administration has determined that this bill has minimal or no impact on small business (attached). The Department of Legislative Services (DLS) concurs with this assessment.

Analysis

Bill Summary: The bill codifies Executive Order 01.01.2019.07 by establishing (1) OSM within DoIT; (2) the position of State Chief Information Security Officer (SCISO) to head OSM; and (3) the Maryland Cybersecurity Coordinating Council (MCCC) to advise and assist the SCISO and OSM. The responsibilities for each entity are substantively similar to those enumerated for each entity in the executive order, except the bill grants more direct authority to OSM to defend against and respond to cyber-attacks.

Specifically, if the SCISO determines that there are security vulnerabilities or deficiencies in information systems, OSM must determine and take the actions necessary to correct and remediate the vulnerabilities or deficiencies and may require the applicable information system to be disconnected. Additionally, if the SCISO determines that there is a cybersecurity threat caused by an entity connected to the State-operated telecommunication and computer network that introduces a serious risk to entities connected to that network or the State, OSM must take or direct actions required to mitigate that threat.

Current Law/Background: DoIT and the Secretary of Information Technology are responsible for:

- developing and enforcing 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;
- adopting and enforcing nonvisual access standards to be used in the procurement of IT services, as specified;
- in consultation with the Attorney General, advising and overseeing a consistent cybersecurity strategy for units of State government, as specified;
- advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy; and
- in consultation with the Attorney General, developing guidance on consistent cybersecurity strategies for specified local government entities.

For information on Executive Order 01.01.2019.07, which created OSM, SCISO, and MCCC, recent cyber-attacks affecting State agencies and local governments, and recent legislation and gubernatorial action taken to address cybersecurity issues in the State, please see the **Appendix – Cybersecurity**.

DoIT currently provides full IT services and/or cybersecurity support for more than 30 Executive Branch agencies. Overall, DoIT provides some level of IT support for approximately 100 State agencies. DoIT advises that, by centralizing IT services in this way, the State has realized cost savings through the reduction of IT positions; consolidation of software licensing, training, and applications; and timely replacement and updates of hardware and software.

In addition, the Governor's proposed budget for fiscal 2023 includes $100 million in funding for cybersecurity assessments and enhancements for State agencies.

State Expenditures: Three major components of the bill affect State operations, but none of them is anticipated to materially affect State finances. First, the bill codifies Executive Order 01.01.2019.07, which established OSM, SCISO, and MCCC. For this component of the bill, there is no fiscal effect beyond what is already incurred under the executive order. Regarding the bill's cybersecurity authority for OSM, DoIT advises that it adds clarity to the authority granted under the executive order and is consistent with its current practices regarding the defense against and response to cyber-attacks.

Second, the bill requires each agency and unit of the Executive Branch of State government, by April 1, 2023, to report to the Governor on the IT systems it uses, data it stores, cloud or statistical analysis system solutions it uses, and vendor interconnections that are in place. The vast majority of agencies that responded to a request for information for this fiscal and policy note advise that the bill's requirements are already being met or can be met using existing budgeted resources with operational changes. Two agencies (the University System of Maryland and the Alcohol and Tobacco Commission) advised that additional staff may be needed to provide the information; however, DLS advises that these and other agencies are likely to be able to provide the information using existing budgeted resources or with minimal additional costs.

Third, the bill requires each unit of the Legislative and Judicial branches of State government that uses the State-operated LATA network to annually certify to DoIT their compliance with DoIT's minimum cybersecurity standards. The Judiciary advises it uses DoIT's LATA network and employs a rigorous cybersecurity framework based on National Institute of Standards and Technology best practices, which likely meets DoIT's standards. DLS advises that it and the General Assembly do not currently use DoIT's LATA network and, therefore, are unaffected by the bill. Even so, DLS and the General Assembly employ a rigorous cybersecurity framework that would likely meet DoIT's standards.

Additional Information

Prior Introductions: None.

Designated Cross File: HB 419 (The Speaker, *et al.*) (By Request - Administration) - Health and Government Operations.

Information Source(s): Department of Information Technology; Maryland Institute for Emergency Medical Services Systems; Maryland Department of Aging; Maryland Longitudinal Data System Center; Maryland Department of Emergency Management; Alcohol and Tobacco Commission; Comptroller's Office; Governor's Office; Judiciary (Administrative Office of the Courts); Office of the Public Defender; Maryland State's Attorneys' Association; Maryland State Department of Education; Maryland School for the Deaf; Maryland Higher Education Commission; Maryland State Library Agency; University System of Maryland; St. Mary's College of Maryland; Maryland Center for School Safety; Maryland Department of Agriculture; Department of Budget and Management; Maryland Department of Disabilities; Maryland Department of the Environment; Department of General Services; Maryland Department of Health; Department of Housing and Community Development; Department of Juvenile Services; Maryland Department of Labor; Department of Natural Resources; Maryland Department of Planning; Department of Public Safety and Correctional Services; Department of State Police; Maryland Department of Transportation; Department of Veterans Affairs; State Department of Assessments and Taxation; Maryland State Board of Elections; State Ethics Commission; Maryland Insurance Administration; Maryland State Lottery and Gaming Control Agency; Military Department; Public Service Commission; Department of Legislative Services

Fiscal Note History: First Reader - February 18, 2022
rh/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.

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: State Government – Information Technology – Cybersecurity

BILL NUMBER: SB 390

PREPARED BY: Patrick Mulford

PART A. ECONOMIC IMPACT RATING

This agency estimates that the proposed bill:

__x___ WILL HAVE MINIMAL OR NO ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

OR

___ WILL HAVE A MEANINGFUL ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

PART B. ECONOMIC IMPACT ANALYSIS

No Impact