HB 346

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 346 (Delegate Novotny)
Health and Government Operations

Department of Information Technology - Oversight of Legislative Branch Information Technology

This bill grants the Department of Information Technology (DoIT) oversight authority over the information technology (IT), information systems, and cybersecurity of any agency or unit of the Legislative Branch of State government.

Fiscal Summary

State Effect: General fund expenditures increase, potentially significantly, for the Maryland General Assembly (MGA) and Department of Legislative Services (DLS) to modify their software contracts, IT systems, data management processes, and cybersecurity practices to comply with specified approved DoIT processes and requirements. Reimbursable revenues and expenditures for DoIT increase to the extent that DoIT charges MGA and DLS for services provided. The bill may also violate constitutional separation of powers provisions, as discussed below.

Local Effect: None.

Small Business Effect: None.

Analysis

Bill Summary/Current Law: 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.

Under current law, DoIT has general IT oversight authority for the Executive Branch of State government, and the aforementioned policies, procedures, standards, plans, and guidance developed by DoIT apply to a "unit of State government." The bill includes an agency or a unit of the Legislative Branch of State government to the definition of "unit of State government," thereby granting DoIT oversight authority to manage and guide the IT and cybersecurity of the Legislative Branch of State government and requiring the Legislative Branch to adhere to the policies, procedures, standards, plans, and guidance developed by DoIT.

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 IT issues in the State, please see the **Appendix – Cybersecurity**.

State Fiscal Effect: General fund expenditures increase, potentially significantly, for MGA and DLS to begin compliance with specified approved DoIT processes and requirements. Specifically, DoIT and the Executive Branch of State government use Google services for its operations, whereas MGA and DLS use Microsoft services. Many of MGA's and DLS's programs, including the bill drafting and fiscal notes systems, are designed to work in tandem with Microsoft services and may need to be redeveloped to function with DoIT's Google-based IT infrastructure. Any costs associated with system redevelopment cannot be reliably estimated but are likely significant.

Moreover, it is unclear whether MGA and DLS could continue to house and control their own data management and IT services under the bill. Specifically, DoIT provides IT services to the agencies it oversees through a fee-for-service model where DoIT employees and/or contractors do the work for an agency, with an appropriate fee. To the extent MGA and DLS are required to adhere to this model as well, (1) reimbursable

revenues and expenditures increase correspondingly as the services are provided and (2) general fund expenditures are significantly affected as MGA and DLS modify their operations and begin to pay DoIT for the services provided.

Additional Comments: A letter of opinion provided by the Office of Counsel to the General Assembly for SB 69 of 2021 (similar legislation that also gave DoIT oversight authority over the Legislative Branch, but to a lesser extent than does the bill) advised that DoIT's oversight of Legislative Branch IT likely violates the separation of powers requirement of the Maryland Constitution. Specifically, Article 8 of the Maryland Declaration of Rights states, "[t]hat the Legislative, Executive and Judicial powers of Government ought to be forever separate and distinct from each other; and no person exercising the functions of one of said Departments shall assume or discharge the duties of any other."

Most notably, the letter of opinion discussed the importance of MGA retaining discretion over its own operations, including its IT systems. Further, members of the General Assembly and legislative staff are protected from liability for or inquiry into their legislative activities by an absolute constitutional privilege, and DoIT's oversight of any Legislative Branch system used to store or transmit privileged legislative records likely constitutes a violation of that privilege.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Office of the Attorney General; Department of Legislative Services

Fiscal Note History: First Reader - January 30, 2022
fnu2/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.