Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 235 (Delegate Carey, *et al.*)
Health and Government Operations Education, Health, and Environmental Affairs

State Government - Department of Information Technology - Cybersecurity

This bill expands the responsibilities of the Secretary of Information Technology to include advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy and, in consultation with the Attorney General, (1) advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions of higher education, and (2) developing guidance on consistent cybersecurity strategies for counties, municipal corporations, school districts, and all other political subdivisions of the State. None of the Secretary's new responsibilities may be construed as establishing a mandate for any of these local government entities.

Fiscal Summary

State Effect: The Department of Information Technology (DoIT) can handle the bill's requirements using existing budgeted resources, as discussed below. The Attorney General's Office, Legislature, and Judiciary can continue to consult with DoIT using existing resources.

Local Effect: No direct effect on local governmental finances; local governmental entities may elect to implement or not implement cybersecurity-related guidance provided by DoIT.

Small Business Effect: None.

Analysis

Bill Summary: "Cybersecurity" means processes or capabilities wherein systems, communications, and information are protected and defended against damage,

unauthorized use or modification, and exploitation. "Cybersecurity strategy" means a vision, a plan of action, or guiding principles.

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

- developing and enforcing information technology (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; and
- adopting and enforcing nonvisual access standards to be used in the procurement of IT services, as specified.

The following agencies are exempt from oversight by DoIT:

- public institutions of education for academic or research purposes;
- the Maryland Port Administration (MPA);
- the University System of Maryland (USM);
- St. Mary's College of Maryland;
- Morgan State University; and
- the Maryland Stadium Authority.

Background: DoIT currently provides full IT services for 31 Executive Branch agencies and cybersecurity support for 38 Executive Branch agencies. Overall, DoIT provides some level of IT support for approximately 100 State agencies. DoIT advises that the cybersecurity support it provides to State agencies costs about $4.0 million annually.

In fiscal 2020, DoIT received $5.0 million in general funds to begin performing cybersecurity assessments on the State agencies it oversees. DoIT plans to use the funding to assess and test 50 of the State's approximately 1,000 applications.

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

State Fiscal Effect: DoIT currently advises and oversees most State agencies with regards to their cybersecurity strategies and systems and has recently developed a State of Maryland Information Technology Security Manual to guide cybersecurity practices in the State, as discussed in the appendix. DoIT does not, however, directly provide any similar

cybersecurity services for counties, municipal corporations, school districts, or other political subdivisions of the State at this time. Even so, DoIT can likely meet the bill's requirements at little to no cost by modifying its existing cybersecurity manual, if necessary, and providing it to these local government entities.

This analysis assumes that DoIT's oversight of the cybersecurity strategy for State agencies specifically exempt from other DoIT oversight (MPA, USM, *etc*.) is merely providing those agencies with the manual that has already been developed and being available for advice and consultation. Thus, DoIT is already meeting the bill's requirement that it oversee a consistent cybersecurity strategy for State agencies, including advising and consulting with the Legislative and Judicial branches. However, to the extent that the bill is interpreted to require DoIT to more closely oversee the cybersecurity strategies of agencies that are currently exempt from its oversight, reimbursable revenues and expenditures for DoIT increase as it provides services for those agencies as well.

Additional Information

Prior Introductions: None.

Designated Cross File: SB 120 (Senator Lee) - Education, Health, and Environmental Affairs.

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

Fiscal Note History: First Reader - January 17, 2020
rh/mcr Third Reader - March 16, 2020
Revised - Amendment(s) - March 16, 2020

Analysis by: Richard L. Duncan

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 (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.