HB 1183

Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
Third Reader

House Bill 1183 (Chair, Health and Government Operations Committee)(By Request - Departmental - Information Technology)

Health and Government Operations Rules

State Government - Information Technology - Cybersecurity

This departmental bill codifies Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative. By April 1, 2021, 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: DoIT 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) the Office of Security Management (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.

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; 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;
- the University System of Maryland;
- St. Mary's College of Maryland;
- Morgan State University; and
- the Maryland Stadium Authority.

Background:

Maryland Cyber Defense Initiative and Department of Information Technology

For more information on Executive Order 01.01.2019.07, which created OSM, SCISO, and MCCC, and cybersecurity issues in the State and across the nation, please see the **Appendix – Cybersecurity**.

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.

One Maryland Broadband Network

The One Maryland Broadband Network is a planned 1,294-mile fiber optic broadband network that will link 1,006 government facilities and community "anchor institutions" in every county in the State, while interconnecting and extending three independent networks: networkMaryland, the inter-County Broadband Network (ICBN), and the Maryland Broadband Cooperative (MDBC).

The broadband network networkMaryland is used by many government agencies throughout the State, including the Legislative and Judicial branches of State government; the network is operated by DoIT. ICBN is a publicly run network that provides broadband services to businesses, community institutions, and residents in the cities of Annapolis and Baltimore and Anne Arundel, Baltimore, Carroll, Harford, Howard, Montgomery, and Prince George's counties. MDBC is a publicly run network that provides broadband services to rural areas in the State.

State Expenditures: The bill includes three major components that affect State operations, but none of the components 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 order.

Second, the bill requires each agency and unit of the Executive Branch of State government, by April 1, 2021, 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. Each agency that responded to a request for information for this fiscal and policy note advised that the information can be provided using existing budgeted resources. Other agencies are also likely to be able to provide the information using existing budgeted resources.

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 that it is in compliance with DoIT's minimum cybersecurity standards. The Judiciary advises that it uses DoIT's LATA network and employs a rigorous cybersecurity framework based on National Institute of Standards and Technology best practices that is likely to meet 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: None.

Information Source(s): Department of Information Technology; Department of Commerce; Governor's Office; Judiciary (Administrative Office of the Courts); Department of General Services; Maryland Department of Labor; Department of Public Safety and Correctional Services; Department of State Police; Maryland Department of Transportation; Military Department; Department of Legislative Services

Fiscal Note History: First Reader - March 5, 2020
md/mcr Third Reader - 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 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.

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: State Government - Information Technology - Cybersecurity

BILL NUMBER: HB 1183

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 BUSINESS

OR

___ WILL HAVE MEANINGFUL ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

PART B. ECONOMIC IMPACT ANALYSIS

There will be no economic impact.