Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 348 (Chair, Education, Health, and Environmental Affairs Committee)(By Request - Departmental - Information Technology)

Education, Health, and Environmental Affairs

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, 2022, 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 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: 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 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.

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.

Second, the bill requires each agency and unit of the Executive Branch of State government, by April 1, 2022, 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 advises that the bill's requirements are already being met or can be met using existing budgeted resources with operational changes. 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 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: HB 1183 of 2020 passed the House and was referred to the Senate Rules Committee, but no further action was taken.

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 Budget and Management; Department of General Services; 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 - January 14, 2021
rh/mcr

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 cyberattacks that have taken place in the nation and the State. Globally, in 2019 and 2020, the Center for Strategic and International Studies identified over 200 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. For example, in November 2020, Baltimore County Public Schools' information technology (IT) systems were made unusable by a ransomware attack and the personally identifiable information (PII) of 27.7 million Texas drivers was exposed in a data breach.

In 2019, governments in the State experienced numerous cyberattacks and breaches. Most notably, Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks. Similarly, the Maryland Department of Labor's licensing database was breached, and 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 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.

Legislation enacted in 2020 expands and enhances the cybersecurity protocols that govern the collection, processing, sharing, and disposal of PII by public institutions of higher education in the State beginning on October 1, 2024.

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. While DoIT and the State have been improving their protection of PII, a 2020 legislative audit found additional issues. For example, in one instance PII was not adequately restricted to employees who should have access to it and instead was visible to over 5,000 State employees.

OLA has previously 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 2020 Cost of a Data Breach Report found:

- the average total cost of a data breach in the United States is $8.6 million; and
- customer PII has the highest cost per record at $150. *For illustrative purposes*, costs for Texas could total $4.2 billion, as a result of the 27.7 million breached records discussed above.

These costs include detection of the breach, escalation, notifications, response, and lost business.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures (NCSL) advises that 38 states, the District of Columbia, and Puerto Rico introduced or considered about 280 bills or resolutions that dealt significantly with cybersecurity in 2020. Some of the key cybersecurity issues considered included:

- requiring government agencies to implement training or specific types of security policies and practices and improving incidence 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.

Moreover, NCSL reports that 19 states (including Maryland) adopted or enacted significant cybersecurity-related legislation in 2020. Notably, (1) Delaware granted its Department of Technology and Information the authority to develop and implement a comprehensive security program; (2) Georgia is using funds from its Revenue Shortfall Reserve to enhance cybersecurity technologies; (3) Louisiana enacted 10 pieces of legislation to significantly enhance its cybersecurity framework; and (4) Virginia required its chief information officer to develop and annually update a training program for all state employees in security awareness and in procedures for detecting, assessing, reporting, and addressing information security threats.

Notably, in 2019, 31 states adopted or enacted significant cybersecurity-related legislation. 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 enacted 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: SB 348

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