Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 340 (The Speaker, *et al.*) (By Request - Administration)
Health and Government Operations Education, Health, and Environmental Affairs

State Government - Protection of Information - Revisions (Maryland Data Privacy Act)

This Administration bill expands and enhances the security protocols that govern the collection, processing, sharing, and disposal of personal information by the State (Executive Branch) and local governments. However, the bill excludes (1) public institutions of higher education from its definition of "unit" and hence the bill's requirements as well as other existing requirements related to the protection of personal information and (2) the Office of the Attorney General (OAG) and local government entities from some of the bill's *specific* cybersecurity and best practice requirements. Public institutions of higher education must submit an annual report to the Governor on their cybersecurity activities, as specified. **The reporting requirement for public institutions of higher education terminates December 31, 2024.**

Fiscal Summary

State Effect: General fund expenditures increase for the Department of Information Technology (DoIT) to assist State agencies with coming into compliance with the bill's cybersecurity requirements. DoIT advises that the proposed FY 2021 budget includes $10.0 million to enhance cybersecurity in the State, including implementing the bill's requirements. State expenditures (all funds) increase, in order for some State agencies to comply with the bill's data security requirements, as discussed below. The reporting requirement can be handled using existing resources. Revenues are not affected.

Local Effect: Local government expenditures may increase in order to comply with the data security requirements established by the bill that apply to units of local government, as discussed below. Revenues are not affected.

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. (The attached assessment does not reflect amendments to the bill.)

Analysis

Bill Summary: The bill generally:

- alters and expands the current statutory definition of "personal information," which is redefined as "personally identifiable information" (PII), and makes conforming changes;
- enhances and redefines the reasonable security measures and practices that each affected unit of State or local government must generally use to protect PII and makes conforming changes;
- excludes certain types of data from the bill's requirements; and
- establishes additional responsibilities related to PII for affected units of State government.

A more extensive discussion of the bill's provisions is provided below.

Applicability

The bill's requirements and existing personal information protection requirements apply only to the collection, processing, and sharing of PII by a unit of State or local government. The requirements do not apply to the collection, processing, or sharing of PII for the purposes of (1) public health; (2) public safety; (3) State security; (4) State personnel or retirement and pension system management; or (5) the investigation and prosecution of criminal offenses. Additionally, the requirements do not apply to the sharing of PII between the Maryland Department of Health and any State or federal agency as allowed by law or regulation.

The requirements may not be construed to (1) alter or supersede the Public Information Act; (2) affect the authority of a unit to make determinations regarding the disclosure of public records consistent with the act; or (3) require a unit to provide access to public records not disclosable under the act.

The Secretary of Information Technology may adopt regulations to carry out the bill's requirements.

Personally Identifiable Information and Security Requirements

All requirements that currently apply to "personal information" instead apply to PII. The "reasonable security procedures and practices" that must be used to protect PII are expanded and enhanced to mean protections that align with DoIT's policies and the Federal Information Security Modernization Act (FISMA) of 2014.

"PII" is defined to mean information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information associated with a particular individual, including (in addition to the unique personal identifiers and financial account numbers that are covered under the existing definition of personal information):

- characteristics of classifications protected under federal or State law;
- biometric information, as specified;
- geolocation data;
- Internet or other electronic network activity information, as specified; and
- information from multiple sources that can be used together or with other information to establish an individual's identity.

"PII" does not include voter registration information, information publicly disclosed by the individual without being under duress or coercion, or data rendered anonymous in a specified manner.

Additional Responsibilities for Units of State and Local Government

OAG and units of local government must continue to use reasonable security procedures and practices to protect PII under the bill; however, they are not required to do so using the same processes and systems specified for units of State government. Except for OAG and local governments, the bill requires agencies to, among other requirements:

- comply with standards and guidelines established by DoIT to ensure that the security of all information systems and applications is managed through State-specified risk management framework, as specified;
- implement specified best practices related to PII and data protection;
- share specified information with an individual regarding the unit's legal authority to collect the information;
- establish a process for an individual to access specified information concerning his or her own PII, as specified; and
- provide specified notice to an individual when the unit intends to share that individual's PII.

The bill imposes additional requirements on units of State and local government, but exempts OAG and local governments from some requirements. For example, all units of State and local government are required to undertake activities comprising the collection, processing, and sharing of PII in good faith, but a unit of State government other than OAG and units of local government must also adopt a privacy governance and risk management program as a best practice to meet this requirement. In meeting the broad data security requirements that apply to them, OAG or a unit of local government may choose

to employ the processes, systems, and best practices required of other units of State government, but they are not generally required to do so under the bill.

Reporting Requirements for Institutions of Higher Education

The bill exempts public institutions of higher education from both the bill's requirements and existing laws governing the protection of PII by government agencies. Instead, by December 1, 2020, and each year thereafter through 2024, each public institution of higher education must submit a report to the Governor that includes (1) a summary of the status of the implementation of any data privacy framework; (2) a description of any barriers or defects to implementation and solutions; (3) the number and disposition of reported breaches, if any; and (4) updates to project cost estimates.

Current Law:

Protection of Personal Information

Chapter 304 of 2013 requires a unit of State or local government (except for the Legislative and Judicial branches of State government) that collects an individual's personal information to implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. Similarly, a unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices.

"Reasonable security procedures and practices" means data security procedures and practices developed, in good faith, and set forth in a written information security policy. "Personal information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- a Social Security number;
- a driver's license number, State identification card number, or other individual identification number issued by a unit of State government;
- a passport number or other identification number issued by the United States government;
- an individual Taxpayer Identification Number; or
- a financial or other account number, credit card number, or credit card number that (in combination with a security code, access code, or password) would permit access to an individual's account.

Personal information does not include a voter registration number.

Department of Information Technology

DoIT and the Secretary of Information Technology are, among other things, responsible for (1) developing and enforcing information technology (IT) policies, procedures, and standards; (2) providing technical assistance, advice, and recommendations to any unit of State government; and (3) developing and maintaining a statewide IT master plan. The following agencies/institutions are exempt from oversight by DoIT:

- public institutions of higher education solely for academic or research purposes;
- the Maryland Port Administration;
- University System of Maryland;
- St. Mary's College of Maryland;
- Morgan State University; and
- the Maryland Stadium Authority (exempted by Chapter 150 of 2018).

Background: DoIT has previously advised that there is no strong legal basis established under current law for the protection of PII. The bill, therefore, expands and enhances the State's regulatory framework for collecting, processing, sharing, disposing of, and protecting personal information and requires most State agencies to implement this framework with DoIT's assistance. For more information on cybersecurity issues facing both the State and the nation, please see the **Appendix – Cybersecurity.**

The National Institute of Standards and Technology (NIST) is a nonregulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. For example, NIST's Special Publication 800 series comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities. The publications are developed to address and support the security and privacy needs of U.S. federal government information and information systems.

NIST also plays an important role in the enforcement of FISMA requirements at the federal level. FISMA was initially enacted at the federal level in 2003 and was most recently updated in 2014. FISMA requires NIST to produce several key IT security standards and guidelines, including numerous Federal Information Processing Standards publications.

State Expenditures:

Compliance Costs for State Agencies

Estimated costs for agencies to comply with the bill's requirements generally fall into two broad categories.

- The majority of State agencies advise that either (1) they already meet the enhanced security requirements established by the bill or (2) they plan to meet the bill's requirements at little to no cost with assistance from DoIT.
- A small number of agencies, such as the Department of Natural Resources, estimate one-time costs of about $40,000 to $60,000 to upgrade existing equipment and purchase new software licenses.

DLS does not have the technical expertise to assess each agency's current security infrastructure and protocols and, therefore, cannot independently verify their estimates for coming into compliance with the bill. The public four-year institutions of higher education and Baltimore City Community College can submit the annual report using existing budgeted resources.

Department of Information Technology

As previously noted, most State agencies plan to implement the bill's requirements by working with and relying on DoIT. Specifically, the fiscal 2020 operating budget for DoIT included $5 million in general funds for DoIT to enhance cybersecurity in the State and DoIT advises that the Governor's proposed budget for fiscal 2021 includes $10 million in general funds for the same purpose. DoIT plans to use these funds primarily to conduct cybersecurity assessments of State agencies, work to rectify any problems discovered, and assist agencies with implementing the bill. The estimate does not reflect any reimbursable revenues (or expenditures) that may be realized because DoIT plans to assist agencies at no cost to the agencies.

Local Expenditures: As previously discussed, many of the bill's broad data protection requirements apply to local governments while the specific processes, best practices, and systems that must be employed under the bill do not. Even so, some local governments may still experience increased expenditures to comply with the bill's requirements, while others may employ systems that already do so. For example, the Maryland Association of Counties advises that most local governments are able to comply with the bill with negligible or minimal increased costs, while at least one county advises that it will have to upgrade multiple hardware and software.

As previously noted, DLS does not have the technical expertise to assess each local government's current security infrastructure and protocols and, therefore, cannot independently verify their estimates for coming into compliance with the bill. Local community colleges can submit the annual report with existing resources.

Additional Information

Prior Introductions: House Bill 716 of 2019, a similar bill, passed both the House and Senate with amendments, but differences between the bills were not reconciled.

Designated Cross File: SB 274 (The President, *et al.*) (By Request - Administration) - Education, Health, and Environmental Affairs.

Information Source(s): Department of Information Technology; Maryland Department of Agriculture; Baltimore City Community College; Department of Commerce; Department of Budget and Management; Department of Human Services; Department of Natural Resources; Department of Housing and Community Development; Maryland Department of Disabilities; Maryland Department of Health; Department of Juvenile Services; Maryland Department of Labor; Maryland Department of Aging; State Retirement Agency; Department of Public Safety and Correctional Services; Maryland Department of Transportation; University System of Maryland; Department of Veterans Affairs; Anne Arundel, Charles, Frederick, Montgomery, and Somerset counties; Maryland Association of Counties; City of Havre de Grace; Department of Legislative Services

Fiscal Note History: First Reader - February 11, 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 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 - Protection of Information - Revisions (Maryland Data Privacy Act)**

BILL NUMBER: HB 340 / SB 274

PREPARED BY: Governor's Legislative Office

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