HB 716

Department of Legislative Services

Maryland General Assembly
2019 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 716 (Chair, Health and Government Operations Committee)(By Request - Departmental - Information Technology)

Health and Government Operations | Education, Health, and Environmental Affairs

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

This departmental bill expands and enhances the regulatory framework that governs the collection, processing, sharing, disposal, and protection of personal information by the State (Executive Branch) and local governments. The bill excludes the Office of the Attorney General from the enhanced cybersecurity requirements and delays application to the University System of Maryland (USM) until fiscal 2022, when USM must implement the same cybersecurity requirements that apply to other agencies.

Fiscal Summary

State Effect: General fund expenditures increase by as much as $1.1 million in FY 2020 for the Department of Information Technology (DoIT) to assist State agencies with coming into compliance with the bill's cybersecurity requirements. The FY 2020 budget includes $5.0 million to enhance cybersecurity in the State, including implementing the bill's requirements. State expenditures (all funds) increase, potentially significantly in some cases, in order for some State agencies to comply with the bill's data security requirements, as discussed below; some costs are ongoing. Revenues are not affected.

Local Effect: Local government expenditures increase, potentially significantly, in order to comply with the data security requirements established by the bill, which apply to units of local government. Revenues are not affected.

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. (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" to be "personally identifiable information" (PII) and makes conforming changes;
- enhances and redefines the reasonable security measures and practices that a unit of State or local government must use to protect PII and makes conforming changes;
- excludes certain types of data from the bill's requirements;
- establishes numerous additional responsibilities related to PII for units of State and local government; and
- maintains current cybersecurity requirements and procedures for USM through June 30, 2021.

A more extensive discussion of the bill's provisions can be found below.

Applicability

The bill's 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 exclusively for the purposes of (1) public health; (2) public safety; (3) State security; or (4) the investigation and prosecution of criminal offenses.

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

The bill requires a unit of State or local government to:

- comply with standards and guidelines, including specified Federal Information Processing Standards (FIPS) and the National Institute of Standards and Technology (NIST) Special Publication 800 series, to ensure that security of all information systems and applications is managed through a NIST 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.

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;
- USM;
- St. Mary's College of Maryland;
- Morgan State University; and
- the Maryland Stadium Authority (exempted by Chapter 150 of 2018).

DoIT currently provides full IT services for 31 Executive Branch agencies and website support for 37 Executive Branch agencies.

Background: DoIT advises 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 State agencies to implement this framework with DoIT's assistance.

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 (SP) 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 FIPS publications.

State Expenditures:

Compliance Costs for State Agencies and Local Governments

With the exception of the Maryland Department of Transportation (MDOT), estimated costs for agencies to comply with the bill's requirements generally fall into the following three 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, as discussed below.

- A small number of agencies, including the Maryland Insurance Administration and the Department of Natural Resources, estimate one-time costs of about $100,000 to upgrade existing equipment and purchase new software licenses.

- Most of the State's public higher education institutions (specifically, the constituent institutions of USM, St. Mary's College of Maryland, and Baltimore City Community College) estimate *ongoing* costs approaching or exceeding $1.0 million annually for each institution; such costs generally reflect additional permanent staff and related system maintenance. In some cases, significant one-time technology costs, such as the purchase of new software and/or entirely new IT systems, are also necessary. For USM, these costs are not incurred until fiscal 2022.

MDOT advises that its costs include (1) one-time system upgrades of $200,000 and (2) ongoing costs of $420,000 for yearly audits to ensure compliance with the bill.

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.

Department of Information Technology – Contractual Staff

As previously noted, most State agencies plan to implement the bill's requirements by working with and relying on DoIT; for those agencies that comply with current security requirements, DoIT plans to provide this assistance free of charge. Therefore, DoIT requires temporary contractual staff to assist agencies during the transition period. For purposes of this analysis, it is assumed that the contractual staff are needed for a nine-month period during fiscal 2020; however, DoIT advises that the staff may be needed for a longer period of time.

Accordingly, general fund expenditures for DoIT increase by $1.1 million in fiscal 2020, which reflects the cost of hiring four contractual programmers and four contractual business analysts to assist agencies. The estimate also includes a one-time cost of $250,000 to purchase additional IT equipment needed under the bill.

Contractual Positions	8.0
Salaries and Fringe Benefits	$819,900
One-time Equipment Costs	250,000
Operating Expenses	42,870
Total FY 2020 DoIT Expenditures	**$1,112,770**

This estimate does not include any health insurance costs that could be incurred for specified contractual employees under the State's implementation of the federal Patient Protection and Affordable Care Act. To the extent that agencies require less support from DoIT than anticipated to come into compliance, expenditures may be less.

The estimate for DoIT's costs under the bill assumes general fund support, consistent with the fiscal 2020 operating budget for DoIT. The budget includes $5.0 million in general funds to enhance cybersecurity in the State, a portion of which is anticipated to be used to implement the requirements of the bill. Thus, the estimate does not reflect any reimbursable revenues (or expenditures) that may be realized because DoIT plans to assist agencies free of charge.

Local Expenditures: Similar to the effect on many State agencies, local government expenditures increase, in some cases significantly, in order to comply with the enhanced information security requirements established by the bill. For example, the Maryland Association of Counties advises that, in general, counties have advised that the bill requires the creation of additional IT positions and, on average, $100,000 in one-time costs for new software; however, some counties estimate that significantly higher costs are incurred. In particular, Montgomery County advises that its total costs could exceed $10.0 million.

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.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Information Technology; Maryland Department of Aging; Department of Commerce; Maryland State Department of Education; Maryland Higher Education Commission; Baltimore City Community College; University System of Maryland; Morgan State University; St. Mary's College of Maryland; Department of Budget and Management; Maryland Department of Disabilities; Department of General Services; Maryland Department of Health; Department of Human Services; Department of Juvenile Services; Department of Labor, Licensing, and Regulation; Department of Natural Resources; Maryland Department of Planning; Department of Public Safety and Correctional Services; Board of Public Works; Department of State Police; Maryland Department of Transportation; State Ethics Commission; Maryland Association of Counties; Montgomery County; Maryland Insurance Administration; Department of Legislative Services

Fiscal Note History: First Reader - March 4, 2019
mag/mcr Revised - Updated Information - March 14, 2019
Third Reader - March 29, 2019
Revised - Amendment(s) - March 29, 2019
Revised - Updated Information - March 29, 2019
Revised - Correction - March 29, 2019

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: Maryland Data Privacy Act

BILL NUMBER: HB716

PREPARED BY: Andi Morony

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

To the extent that small business would either have to spend money or act on this legislation-there is no impact. It is important to note however, that there is value in protecting, to the greatest extent possible, all PII. The theft of PII can cost untold amounts of money.