HB 1122

Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 1122 (Delegate Pena-Melnyk, *et al.*)

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

State Government – Protection of Personally Identifiable Information – Public Institutions of Higher Education

This bill expands and enhances the security protocols that govern the collection, processing, sharing, and disposal of personally identifiable information (PII) by public institutions of higher education in the State. **The bill takes effect October 1, 2024.**

Fiscal Summary

State Effect: To comply with the bill's data security requirements, higher education and general fund expenditures increase significantly for the University System of Maryland (USM), Morgan State University (MSU), St. Mary's College of Maryland (SMCM), and Baltimore City Community College (BCCC) beginning as early as FY 2021, as discussed below. Revenues are not affected.

Local Effect: Expenditures increase for local community colleges; as discussed below, significant costs may be incurred before the bill's effective date. Revenues are not affected. **The bill imposes a mandate on a unit of local government.**

Small Business Effect: Potential minimal.

Analysis

Bill Summary: "Public institution of higher education" means the constituent institutions of USM and the University of Maryland Center for Environmental Science, MSU, SMCM, and a community college established under Title 16 of the Education Article (including BCCC).

Applicability

The bill does not apply to PII that:

- is publicly available information that is lawfully made available to the general public from government records;
- an individual has consented to have publicly disseminated or listed;
- is disclosed in accordance with the federal Health Insurance Portability and Accountability Act (except for a medical record that a person may not redisclose pursuant to § 4-302(d) of the Health – General Article);
- is disclosed in accordance with the federal Family Educational Rights and Privacy Act; or
- is clinical information or is information related to sponsored research.

A public institution of higher education must continue to comply with any other requirements of State or federal law relating to the protection of PII.

Personally Identifiable Information

"PII" is defined to mean information that enables the identification of an individual, 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):

- biometric information, as specified;
- geolocation data; and
- Internet or other electronic network activity information, as specified.

Cybersecurity and Protection of Information Systems

The bill requires each public institution of higher education to review and designate systems within the respective institution as systems of record based on specified criteria. The bill establishes numerous technical specifications for the protection of institutions' information systems and PII. Broadly, each public institution of higher education must:

- develop and adopt a privacy governance program to govern each system of record;
- develop and adopt an information security and risk management program for the protection of PII, as specified;
- publish a privacy notice on its website, as specified;
- follow specified procedures when destroying PII records; and

- follow specified procedures when it discovers or is notified of a breach of the security of one of its systems.

Current Law: 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.

Background: For more information on cybersecurity issues facing both the State and the nation, please see the **Appendix – Cybersecurity.**

State/Local Expenditures: USM anticipates significant costs under the bill, with planning and *pre-implementation* costs of $7.3 million to be incurred systemwide over four and a half years (likely beginning in fiscal 2021). The Department of Legislative Services (DLS) advises that it is unclear how USM can comply with the bill if it does not take action well in advance of the bill's October 1, 2024 effective date. Implementation costs spanning over fiscal 2024 and 2025 (when the bill takes effect) are estimated at $12.4 million; ongoing maintenance costs total about $8.9 million annually thereafter. These costs are related to various factors, including:

- additional personnel;
- information technology;
- education and training for employees; and
- contractual services such as electronic erasure of privacy data and paper shredding services.

USM advises that its smaller constituent institutions would work collaboratively and share resources. The larger constituent institutions would work more independently but would look for opportunities to collaborate as well.

The costs above are only related to USM and are assumed to be covered with a combination of higher education and general fund expenditures; additional (likely significant) higher education and general fund expenditures are also anticipated for MSU, SMCM, and BCCC. Local expenditures increase for the 15 local community colleges in Maryland; however, State aid and tuition revenues may be redirected to this purpose as well. In each case, costs are assumed to be incurred prior to the bill's effective date to ensure compliance.

DLS does not have the technical expertise to assess each institution's current security infrastructure and protocols and, therefore, cannot independently verify the cost for each public institution of higher education throughout the State to come into compliance with the bill.

Additional Information

Prior Introductions: None.

Designated Cross File: SB 588 (Senator Kagan) - Education, Health, and Environmental Affairs.

Information Source(s): University System of Maryland; Department of Legislative Services

Fiscal Note History: First Reader - February 11, 2020
rh/ljm Third Reader - April 10, 2020
Revised - Amendment(s) - April 10, 2020

Analysis by: Eric F. Pierce

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.