DOIT_MIKELEAHY_FWA_SB0274
Uploaded by: Chase, Erin
Position: FWA

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

February 13, 2020

The Honorable Paul G. Pinsky, Chair
Education, Health and Environmental Affairs Committee
Miller Senate Office Building, 2 West
Annapolis, MD 21401

Dear Chairman Pinsky:

The Department of Information Technology (DoIT) supports Senate Bill 274 - State Government - Protection of Information - Revisions (Maryland Data Privacy Act) with an amendment. The amendment clarifies the standards and guidelines in which the units of government will need to comply with to ensure that the security of all information systems and applications are managed in a manner that is consistent with the State specified risk management framework.

Within state government, the goal should be to limit the amount of Personally Identifiable Information (PII) collected and ensure Marylanders understand why their information is being collected, for what purposes and how it is being used. Citizens must also have confidence that their government is taking the proper precautions to ensure the confidentiality and integrity of their information. Senate Bill 274 requires compliance with certain standards and guidelines to ensure that all personal data is being collected and managed in a secure manner.

Under this legislation, certain state agencies would be required to collect, process and share PII in a manner that is consistent with the requirements set forth by the Maryland Department of Information Technology, including:

- Identifying and documenting the legal authority for the collection of such data.
- Notifying an individual when PII is being collected and describe the purpose for the collection.
- Implementing reasonable data handling procedures to ensure the confidentiality, integrity, and availability of all PII is maintained.
- Incorporating privacy requirements into agreements with any third parties that handle PII while under contract with the State.
- Ensuring that PII collected is accurate, relevant, timely, and complete.
- Only collecting PII that is relevant to the legally authorized purpose of the collection.
- Allowing the individual access to their PII and allowing them to correct or amend the collected PII and
- Informing the individual or public of the practices and activities regarding the use of their PII including any rights the individual or public has to decline, correct or review the PII.

The Maryland Data Privacy Act modernizes the way state government agencies secure and manage PII. The bill requires agencies to mirror federal procedures for ensuring that PII is protected from unauthorized access, use, modification, or disclosure. Citizens must also be advised whether the disclosure of certain PII is voluntary or required, how that information is shared with third parties, and be provided an opt-out provision when possible. This proposal does not address private industry and broadly excludes uses related to public safety, public health, state security, and the investigation and prosecution of criminal offenses. To the extent that current laws and policies are being followed, there will be no fiscal impact because of this legislation.

For these reasons, the Maryland Department of Information Technology respectfully requests a favorable report on Senate Bill 274 as amended.

Amendment for Senate Bill 274

On page 6 replace line 22 through 29 with :

EACH UNIT SHALL COMPLY WITH STANDARDS AND GUIDELINES SET FORTH BY THE DEPARTMENT OF INFORMATION TECHNOLOGY, TO ENSURE THAT THE SECURITY OF ALL INFORMATION SYSTEMS AND APPLICATIONS IS MANAGED THROUGH STATE SPECIFIED RISK MANAGEMENT FRAMEWORK;

1. THE SYSTEM IS CATEGORIZED BASED ON AN ANALYSIS OF THE STATE SYSTEM CATEGORIZATION CRITERIA ;

GovernorsOffice_ErinChase_FWA_SB0274
Uploaded by: Chase, Erin
Position: FWA

STATE OF MARYLAND
OFFICE OF THE GOVERNOR

LARRY HOGAN
GOVERNOR

STATE HOUSE
100 STATE CIRCLE
ANNAPOLIS, MARYLAND 21401-1925
(410) 974-3901
(TOLL FREE) 1-800-811-8336

TTY USERS CALL VIA MD RELAY

Senate Bill 274 - State Government - Protection of Information - Revisions (Maryland Data Privacy Act)

Position: Support (with Amendments)

Senate Education, Health, and Environment Affairs Committee

February 13, 2020

Testimony By:
Erin Chase, Deputy Legislative Officer, Governor's Legislative Office

Chair Pinsky, Vice Chair Kagan, and Members of the Senate Education, Health, and Environmental Affairs Committee:

The Hogan-Rutherford Administration understands and recognizes the importance of strengthening our cybersecurity, privacy, and data governance policies, and is committed to protecting the personally identifiable information (PII) of Maryland's citizens and those who do business with the state. When citizens interact with the state government, they have the expectation that their PII, such as social security numbers, bank account numbers, and biometric information, is being handled with the utmost confidentiality and integrity, and we have an obligation to uphold that trust. Senate Bill 274 will update our statute to clearly provide for the protections of PII that our citizens deserve.

Currently, Maryland's statute does not provide a strong legal basis for the protection of an individual's PII. State agencies use their own frameworks to protect data, and while many of these agencies may employ best practices for addressing privacy, it is important that the statute be updated to streamline all standards and guidance to ensure that data is being uniformly protected across the executive branch of state government. The state is ultimately accountable and responsible for the protection of this private and sensitive information, and it is crucial that our statute accurately reflect that.

The Maryland Data Privacy Act will amend and strengthen Maryland's law by better defining personally identifiable information, and require the implementation and compliance with standards that mirror federal policies and procedures, which would reflect current best practices. These practices will provide individuals with insight into how and why their PII is being collected and used. Agencies will be required to institute policies such as identifying and documenting the legal authority for the collection of such data; notifying the individual when PII is being collected; describing the purpose for collection; and informing the individual or public of the practices and activities regarding the use of their PII including any rights the individual or public has to decline, correct or review the PII. This bill will prove to be an effective tool to help state agencies best secure and manage PII while also providing transparency to citizens so that they better understand how and why their data is being used.

As we continue to bolster our state's position on issues relating to cybersecurity, Maryland must have a consistent and responsible law that sets one standard to provide the assurance to our constituents that their information is being collected, stored, shared, and disposed of in a secure and uniform manner.

For these reasons, the Administration respectfully requests a favorable report on Senate Bill 274.

For additional information, please contact Erin Chase at erin.chase1@maryland.gov or 410-974-3336.

Proposed Amendment:

On page 6 replace lines 22 through 29 with:
EACH UNIT SHALL COMPLY WITH STANDARDS AND GUIDELINES SET FORTH BY THE DEPARTMENT OF INFORMATION TECHNOLOGY, TO ENSURE THAT THE SECURITY OF ALL INFORMATION SYSTEMS AND APPLICATIONS IS MANAGED THROUGH STATE SPECIFIED RISK MANAGEMENT FRAMEWORK;

1. THE SYSTEM IS CATEGORIZED BASED ON AN ANALYSIS OF THE STATE SYSTEM CATEGORIZATION CRITERIA;

MACC_Klimczak_FWA_SB0274
Uploaded by: Klimczak, Craig
Position: FWA

Senate Education, Health & Environmental Affairs Committee

TESTIMONY
Submitted by Dr. Craig Klimczak, Chair of the Maryland Community College's Technology Officers and
Chief Information Officer for the Community College of Baltimore County CCBC)

cklimczak@ccbcmd.edu

February 13, 2020

BILL: SB 274 – State Government – Protection of Information – Revisions (Maryland Data Privacy Act)

POSITION: Request that public institutions of higher education be excluded from the provisions of this subtitle and its companion bill in the house. Note that the University System of Maryland has been excluded in this subtitle which is subject to same federal laws and regulations as other public institutions of higher education (IHE) in Maryland. Community colleges and other public institutions of higher education must deal with the same complexities and systems that impact the University System of Maryland.

RATIONALE:

- Public institutions of higher education have been subject to and held in compliance to privacy legislation for many years by the federal statue Family Educational Rights and Privacy Act (FERPA) passed in 1974. This law and its associated federal regulation provide rules for disclosure of personally identifiable information to third parties, issues of consent, and issues of accuracy and correction.
- Public institutions of higher education operate a complex web of systems and solutions pertinent to the delivery of instruction and education that are unique in comparison to traditional governmental record systems. Institutions of higher education operate learning management systems and social portals to deliver instruction that create the social atmosphere of attending school with a cohort of students. Certain privacy provisions that limit exchange of PII in these bills would make cohort-based instruction difficult if not impossible. Further, institutions of higher education will have to implement systems, processes, people and changes to instructional pedagogy to accommodate potential student requests to Opt-Out of sharing personally identifiable information. Institutions of higher education need provisions that allow for the creation of governance and due process procedures to adjudicate privacy requests.
- Public institutions of higher education are subject to security and privacy regulations from the US Department of Education who by contractual obligation applies the privacy and data security standards of Gramm-Leach-Bliley-Act to higher education institutions

that receive Title IV funds. The Department of Education recently added audit requirements that assess an institution of higher education's compliance with these provisions. Specifically, the Department of Education has instructed audit firms to audit:

- Determine whether the institutions of higher education designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.
- Verify that the institutions of higher education has designated an individual to coordinate the information security program.
- Obtain the institutions of higher education risk assessment and verify that it addresses the three required areas noted in 16 CFR 314.4 (b).
- Obtain the documentation created by the institutions of higher education that aligns each safeguard with each risk identified from the risk assessment specified above, verifying that the institutions of higher education has identified a safeguard for each risk.

While the Maryland Community Colleges' Technology Officers agree with the intent of the legislation, additional state statues could create confusion and potentially create conflicts in interpretation. Further some of the requirements would be onerous and costly to community colleges as they would require additional and somewhat redundant standards of compliance above what community colleges already provide for FERPA, GLBA, and related. Most community colleges have not had a chance to analyze the impact of this bill or estimate the cost to be compliant. However, any increase will have major effect on the budgets for community colleges.

The Maryland Community Colleges' Technology Officers apologizes that we weren't aware of other data security legislation that has been reviewed by this Committee such as SB0120/HB0235. Existing statutes require, that community colleges report to the MD OAG and Department of Education, in the event of a breach of PII. We request for the same reasons mentioned above that public institutions of higher education be excluded from SB0120/HB0235 as well.

In addition, yesterday this committee heard testimony on SB 588 regarding protection of personally identifiable information; however, it too, exempts the University System of Maryland from the provisions of 10-1301 thru 10-1304 and creates a new sub-title 10-13A for the University System of Maryland. We ask that you place all public institutions of higher education under the language inserted for System schools. This alternative language is more consistent with federal legislation and regulations currently being imposed on public institutions of higher education.

Should this act include public institutions of higher education, the Maryland Community Colleges' Technology Officers request the date the act takes effect be moved into the future to allow time for institutions to modify and adjust systems in accordance with the proposed law. We request that the act take effect no sooner that October 1, 2022.