House Health & Government Operations 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 25, 2020

BILL: HB 340 – State Government – Protection of Information – Revisions (Maryland Data Privacy Act)

POSITION: Favorable with Amendments

Request that public institutions of higher education be excluded from the provisions of this subtitle and its companion bill in the Senate. The University System of Maryland has been excluded in this subtitle through this bill. Concurrently, the University System of Maryland has been inserted into a parallel privacy and security bill HB1122. Community colleges, which are subject to the same federal laws and regulations as University System of Maryland, request to be inserted into HB1122. The Senate sponsor of the companion measure to HB1122 (SB 588) has offered amendments to include community colleges.

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 personally identifiable information 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 (GLBA) 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, audit firms are instructed to:
    - Verify that the institutions of higher education have 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).
        - Employee training and management,
        - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and
        - Detecting, preventing, and responding to attacks, intrusions, or other system failures
    - 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 have 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 and privacy legislation that is under consideration such as HB235/SB120. Existing statutes require, that community colleges report to the MD Office of Attorney General 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 HB235/SB120 as well.

In closing, this committee will hear testimony on HB1122 regarding protection of personally identifiable information. It also 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 provisions inserted for System schools. Similarly, the provisions in HB1122 protects the privacy of Maryland citizens and is more consistent with federal legislation and regulations currently imposed on public institutions of higher education.

Should HB340 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 HB340 take effect no sooner that October 1, 2022 as is specified in HB1122.