**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.