

**JOINT COMMITTEE ON CYBERSECURITY, INFORMATION
TECHNOLOGY, AND BIOTECHNOLOGY JOINT COMMITTEE ON
CYBERSECURITY, INFORMATION TECHNOLOGY, AND
BIOTECHNOLOGY**
2023 Interim

State Government Article, Section 2-10A-13(f)

JOINT COMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY

December 15, 2023



THE MARYLAND GENERAL ASSEMBLY
ANNAPOLIS, MARYLAND 21401-1991

JOINT COMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY

December 15, 2023

The Honorable Bill Ferguson, Co-Chair
The Honorable Adrienne A. Jones, Co-Chair
Members of the Legislative Policy Committee

Dear President Ferguson, Speaker Jones, and Members:

The Joint Committee on Cybersecurity, Information Technology, and Biotechnology respectfully submits this summary report of its 2023 interim activities. The joint committee held three meetings primarily focused on artificial intelligence (AI).

At the first meeting, held on June 21, the joint committee received (1) an introduction and overview on AI issues from professors from the University of Maryland, Baltimore County (UMBC); (2) a summary of regulatory actions and strategies from other nations and states to govern AI, presented by the University of Maryland Center for Health and Homeland Security (CHHS); and (3) examples of specific AI-related research conducted by UMBC professors.

- The first panel of UMBC professors discussed the history of AI, beginning with the philosophical question of what constitutes intelligence; the various types of AI currently in use and development, including generative AI systems which have grown significantly in popularity over the last year (*e.g.*, ChatGPT); the basics of machine learning, which fuels many AI systems; and examples of how AI could be used, including in medicine and addressing climate change.
- Second, representatives from CHHS provided an overview of state regulatory actions related to AI. Many states regulate AI by (1) creating a task force or committee to make recommendations or provide oversight; (2) prohibiting or limiting the use of AI in certain industries or sectors; (3) requiring oversight and/or assessments for AI use; and/or (4) creating a cause of action for citizens to seek remedies from AI-related harms.
- Finally, professors from UMBC discussed real-world examples of research that they conducted relating to AI. The research topics included natural language processing (to help

December 15, 2023

Page 2

AI better understand and recognize language patterns) and robotics (to enhance quality and more complex automation).

At the second meeting, held on October 25, the joint committee delved into how AI is used or could be used in various policy areas; including education, consumer protection and constituent services; labor; disinformation and misinformation in elections; and general governance of AI. Panelists included state agencies, professors, and private-sector experts. The panelists for how AI and education intersect presented on the following.

- States should promote training of K-12 teachers in the use of AI in the classroom. The University of Connecticut's Center for Excellence in Teaching and Learning has taken the lead on developing professional resources for teachers.
- The U.S. Secretary of Education plans to create and release an AI toolkit for education leaders in the coming year and will implement recommendations from the Department's "Artificial Intelligence and the Future of Teaching and Learning" report.
- President Joseph R. Biden's October 30, 2023, executive order calls for the Secretary of Education to create resources that address safe, responsible, and nondiscriminatory uses of AI in education in consultation with relevant stakeholders.

The panelists regarding AI and consumer protection presented on the following.

- Consumer data privacy laws, including specified comprehensive laws enacted in California, Colorado, Connecticut, Utah, and Virginia, along with the European Union's General Data Protection Regulation, provide useful protections for certain existing and emerging AI applications, particularly with facial recognition applications. Consumer data privacy laws are even more important now with the accelerated growth of AI.
- Inventories of existing AI used by government entities, procurement rules for AI and products that include AI, and impact assessments to identify potential risks and harms caused by AI are all common foci for states beginning to regulate AI to protect consumers.
- Transparency is an important issue for consumers and remains a top priority for regulators. There is no standardized method (yet) for labeling content as AI generated, in addition to there being no tool that uses such labels that enable consumers to identify AI-generated content. However, several pending bills in Congress are calling for these to be developed.

The panelists regarding AI and labor-related issues presented on the following.

- States have an opportunity to implement minimum standards for private industry use of AI that outlines appropriate risk-based approaches. States should be cognizant of creating concrete governance approaches that recognize roles and leverage tested accountability tools.

December 15, 2023

Page 3

- Policymakers should examine regulation in electronic surveillance and automated management systems regulation, along with automated job tasks and automated employment decisions. Some practices policymakers should consider when discussing regulation of electronic surveillance and automated management systems in the workplace include (1) data minimization; (2) harm prevention; (3) transparency; and (4) auditing.
- The use of AI and its effects on the economy may be larger than many expect. Also, the effects may not be limited to the technology sector but may disrupt operations in the greater economy.

The panelists regarding AI and elections presented on the following.

- The State should be aware of prior misinformation and disinformation campaigns that were allowed to spread and consider avenues to educate the public, when appropriate. Some experts recommend the State take a proactive approach to misinformation and disinformation campaigns, rather than being reactive.

The panelists regarding AI and governance presented on the following.

- AI may have a larger impact on the economy than past innovations, such as electricity and personal computers.
- Governance structures vary among the few states that already regulate AI. Some states established advisory boards while others empowered public bodies to regulate AI directly. In addition, some states are considering the regulation of specific AI issues (such as AI facial recognition by law-enforcement) while others are considering regulating more broadly.
- Notably, Connecticut took a hybrid approach by establishing a 21-member working group that includes both advisory and regulatory authorities. Colorado established an AI facial recognition task force, and Washington proposed an Algorithmic Accountability Review Board to require agencies to meet certain requirements for any automated decision-making systems used by the agencies.

At its final meeting, held on November 29, the joint committee heard from presenters regarding (1) an update on the modernization efforts involving the ONESTOP and the Financial Management Information System (FMIS) software projects; (2) an update on the State's use of AI; (3) an update on the State's cybersecurity posture; and (4) a briefing on the nexus of cybersecurity and AI.

- Representatives from the Department of Information Technology (DoIT), the Department of Legislative Services, the Office of the Comptroller, and System Automation provided an update on the status of the ONESTOP and FMIS projects. DoIT acknowledged that the project is still in development but also recognized the ONESTOP system may not be the "forever answer" for the State. The Office of the Comptroller indicated that it is currently between program planning and strategy, and solicitation and planning, for the FMIS

project. System Automation provided best practices for similar systems in other states that Maryland should consider as it improves ONESTOP and FMIS. DoIT was asked to provide a timeline and budget for its modernization plans.

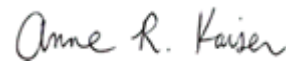
- Representatives from DoIT and McKinsey and Company indicated that the State should begin to plan for the foundational work necessary to ensure the State's responsible and productive use of AI. This includes establishing ethical guardrails on the use of AI, determining the risk of generative AI use on a case-by-case basis, and effectively managing risk associated with AI by establishing robust governance policies and implementing effective controls/regulatory compliance standards. DoIT was asked to provide a timeline and budget for implementation of AI governance and policies.
- Representatives from DoIT discussed the State's cybersecurity posture, including (1) preliminary findings from cybersecurity assessments of State agencies; (2) developments in partnerships with the Maryland National Guard and State colleges and universities; (3) considerations to expand Office of Security Management services; and (4) additional cybersecurity support available to K-12 systems. DoIT was asked to provide a timeline and budget for the remediation of the cybersecurity assessments.
- Representatives from RSM US LLP, SAF.AI Inc., and Palo Alto Networks Inc. discussed how AI affects cybersecurity, both as it is used by hackers and to defend against hackers. While AI can be helpful in identifying and resolving certain cybersecurity threats, bad actors also have access to AI systems that allow them to execute a greater number of attacks that are also more sophisticated. Generally, the speakers indicated that AI creates a new layer of complexity for handling cyber threats to critical systems.

Please contact us if you have any questions concerning the joint committee's activities.

Respectfully submitted,



Katie Fry Hester
Senate Chair



Anne R. Kaiser
House Chair

KFH:ARK/RD/bal

cc: Victoria L. Gruber
Ryan Bishop
Sally Robb
Jeremy Baker