

THE MARYLAND GENERAL ASSEMBLY
ANNAPOLIS, MARYLAND 21401

JOINT COMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND BIOTECHNOLOGY

December 18, 2019

The Honorable Thomas V. Mike Miller, Jr., Co-chair
The Honorable Adrienne A. Jones, Co-chair
Members of the Legislative Policy Committee

Ladies and Gentlemen:

The Joint Committee on Cybersecurity, Information Technology (IT), and Biotechnology respectfully submits this summary report of its 2019 interim activities. The committee held three meetings during the 2019 interim covering a range of issues related to its charge.

At the first meeting, held June 26, the committee was briefed on the following topics.

- Todd Tucker from the Technology Business Management (TBM) Council, a national nonprofit professional organization, discussed the TBM information technology management strategy. TBM is used by numerous private companies, as well as state-level and federal agencies to cost-effectively manage its IT systems.
- The Department of Information Technology (DoIT) presented on its goals for 2019 and future years, which included standardizing cybersecurity governance across all State agencies, establishing a one-stop portal in the State for license and permit applications, and further developing the State-owned internet service, Network Maryland. DoIT also discussed the newly created State Chief Information Security Officer (CISO) position and its responsibilities. The National Association of State CISOs further discussed the important role played by state CISOs and the importance of comprehensive cybersecurity practices.
- The Maryland Emergency Management Agency (MEMA) and National Guard discussed the State's response and recovery process during and after cyberattacks, and their agencies roles in that process. MEMA advised that its role is primarily one of ensuring coordination between first responders and other involved parties. The National Guard advised that it responds when requested to do so by the Governor, and is primarily involved in triage and stabilization of systems after a cyberattack takes place.

December 18, 2019

Page 2

- Richard Forno, Director of the University of Maryland, Baltimore County's graduate cybersecurity program, discussed the program's goals and accomplishments in training the next generation of cybersecurity experts and working to connect those students to State agencies.
- A panel of experts working for private companies in the cybersecurity industry shared a variety of insights and advice for the committee and emphasized the importance of comprehensive cybersecurity practices by discussing recent incidents experienced throughout the State. The centralization of IT systems and administration was a key concern among the experts.

At the second meeting, held October 2, the committee was briefed on the following topics.

- A panel of representatives from the Georgetown University Hospital, University of Maryland School of Medicine, and University of Maryland Children's Hospital presented information on the link between teen and child mental health problems and internet use. The speakers discussed strategies for caregivers to mitigate the risks, including limiting internet use, monitoring content, and using the internet with your teen/child to build healthy internet usage habits.
- Mike Galiazzo, President of the Regional Manufacturing Institute of Maryland, and LaToya Staten, Chief Strategy Officer of Connected2Tech, discussed the future of work and workforce development. Both speakers emphasized that new technologies, including automation, are changing what work will look like in the future. Most notably, entry-level jobs are beginning to require more and more technical skills, as current entry-level jobs (such as retail work) are automated. The speakers made policy recommendations for the committee, including trying to anticipate new technologies and address problems they may cause before the problems arise and supporting workforce development programs through various means.
- The Southern Maryland Agricultural Development Commission, Maryland Farm Bureau, and Mid-Atlantic Farm Credit presented on the future of agriculture. The speakers emphasized the importance of new technologies to farming, the prominence of automation in the industry, and the importance of ensuring farmers have access to credit and loans to afford the new technologies.
- Martin Rosendale, Chief Executive Officer of the Maryland Technology Council, presented on the importance and future of biotechnology, as well as what the State can do to assist the biotechnology industry, including supporting innovation in the industry, ensuring access to capital through incentives and acceleration programs, encouraging workforce development programs, and supporting the construction of infrastructure, such as lab space.

December 18, 2019

Page 3

At the third meeting, held December 4, the committee was briefed on the following topics.

- Mike Thielke, from the F3 Tech Accelerator Program, and Aaron Ault, senior research engineer for the Open Ag Technology Center at Purdue University, discussed the importance of data and the automation of data-related processes for the farming industry. They further discussed the technology strategies to make this possible, including new strategies to securely transport and analyze data and open source software.
- Alec Ross, author of the “Industries of the Future,” and former senior advisor for innovation to Secretary of State Hillary Clinton, discussed the effect that automation, artificial intelligence, and robotics will have on the nation’s work and workforce in the coming years. He described the skills that will be less necessary for the workforce to have (such as manual dexterity skills), the skills that will be more necessary for the workforce to have (such as critical thinking and emotional intelligence), and made suggestions on how Maryland legislators can prepare for these changes with the development of technology.
- Representatives from DoIT answered questions from the committee concerning what they as an agency can do and are doing to keep State agencies and other entities in the State (such as public utilities) safe from cyberattack. Among other things, DoIT advised that it cannot do much to help or assist non-State agencies unless they are asked to do so and that it is working on departmental legislation to address various issues with the protection of State data.
- Maryland Technology Development Corporation (TEDCO) and some of its entrepreneurial partners discussed the process by which, TEDCO directly supports technology companies in the State. In addition, TEDCO agreed to survey its partners and entrepreneurs to get a better sense of what the legislature can do to improve the business climate for tech companies in the State.

While the joint committee are still reviewing the input gathered through these three hearings, the key insights and recommendations for consideration going into the 2020 session include the following.

State Cybersecurity

Through numerous conversations with DoIT, the joint committee received a better understanding of the State’s overall cybersecurity posture. These insights are collected in a questions and answers document which the joint committee can provide upon request. The State has made a number of key improvements; however, it is still hampered by key variables, including (1) that only half of state agencies work with DoIT, Legacy systems across the state agencies present vulnerabilities, and the State is significantly under-invested in cybersecurity compared to

December 18, 2019

Page 4

the private sector and other states. Given this context, the joint committee is reviewing legislation to support including:

- statutorily defining the State Chief Information Security Officer (CISO) position and its responsibilities;
- requiring all state agencies using the State-owned internet service to comply with DoIT standards;
- providing incentives for students to connect to the state government through internships and apprenticeship incentives;
- increasing the budget allocation for cybersecurity in accordance with the Cyber Security Council's recommendations and the department's request;
- supporting departmental legislation to address the protection of State data; and
- considering the redaction of specific details of cybersecurity breaches from the publicly available audit reports.

Local Government Cybersecurity

Given the recent cyber-attack on Baltimore City and the economic fallout resulting from the attack, the joint committee was particularly interested in how it could help local governments. Since DoIT is only able to assist non-State agencies when they are asked to do so, and the National Guard only responds when requested to do so by the Governor (and is primarily involved in triage and stabilization after an attack), the joint committee is reviewing legislation to support including:

- encouraging MEMA's coordination role following an attack;
- sharing DoIT products with localities and small businesses, including encouraging local governments to adopt DoIT's cybersecurity policies, security handbook, and 24-hour response plan (which is currently being developed);
- marketing these policies and best practices to small business, potentially with the assistance of the Maryland Small Business Development Center.

Workforce Development in Cybersecurity, IT & Biotechnology

New technologies including automation, robotics, and artificial intelligence are changing what work will look like in the future and it is the State's responsibility to ensure that its students are employable. Most notably, entry-level jobs are beginning to require more and more technical skills, as current entry-level jobs (such as retail work) are becoming more automated. Given this context and the importance of the recommendations of the Commission on Innovation and Excellence in Education (Kirwan Commission) this year, the joint committee is considering how the state can:

- best anticipate new technologies and address potential workforce problems before they arise;
- encourage the development of workforce skills less susceptible to automation (such as analytical and emotional skills);
- ensure our students have a baseline knowledge of IT and cybersecurity when graduating from high school;
- invest in the development of the local and regional workforce; and
- support innovation across industries (in particular biotechnology, agriculture, and aquaculture through access to capital through credit and loans, acceleration programs, encouraging workforce development programs, and supporting infrastructure, such as lab space).

Education, IT & Cybersecurity

Directly related to workforce development, the joint committee is interested in exploring the link between technology and mental health, especially as it relates to students. This issue is directly relevant to the work of the Kirwan Commission and is changing rapidly given the nature of technology. The joint committee is considering:

- encouraging the collaboration of the Maryland State Department of Education (MSDE) and the Department of Health to study and look for opportunities to encourage the mental health of our kids – in partnership with the University of Maryland School of Medicine;
- finding ways to discourage unhealthy practices (such as cyber bullying);

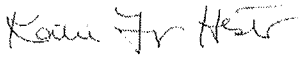
December 18, 2019

Page 6

- finding ways to use technology to support mental health (for example Utah's mental health app for kids which connects them to a variety of resources); and
- developing state-level guidance for caregivers to mitigate the risks, including limiting internet use, monitoring content, and using the internet with your teen/child.

Please contact us or the committee staff, Richard Duncan and Mary Clarke, at (410) 946-5510 if you have any questions concerning the committee's activities.

Respectfully submitted,



Katie Fry Hester
Senate Chair



Michael A. Jackson
House Chair

KFH:MAJ/RLD/mta

cc: Mr. Jake Weissman
Ms. Alexandra M. Hughes
Ms. Victoria L. Gruber
Mr. Ryan Bishop