Meeting Minutes
Maryland Cybersecurity Council
Subcommittee on Education and Workforce Development
Thursday, January 21, 2021
5:00 pm – 6:00 pm
Virtual Public Meeting

Attendance (7/12)
Subcommittee members attending: Senator Katie Fry Hester (chair), Dr. Michel Cukier, Dr. Anupam Joshi, Miheer Khona, Laura Nelson, Rodney Petersen, and Jonathan Prutow.

Other Council members joining: Gregg Smith, Chairman of the Board, Cybersecurity Association of Maryland.

Staff: Howard Barr (Assistant Attorney General and Principal Counsel, DoIT), Nithin Venkatraman (Chief of Staff, Office of Senator Hester), and Dr. Greg von Lehmen (University Maryland Global Campus, Staff to the Maryland Cybersecurity Council)

1. Nithin Venkatraman welcomed the subcommittee members and opened the meeting for Senator Hester, who joined the meeting at about 5:15 pm.
2. The minutes for the 13 November 2020 meeting were called. No changes were requested. The minutes were approved on motions by Dr. Joshi and Mr. Khona.
3. Dr. von Lehmen provided an overview of bills that aligned with the objectives of Council recommendations:
   - SB 69 (Maryland Emergency Management Agency - Cybersecurity Coordination and Operations Office – Establishment)
   - SB 49/HB 38 (Department of Information Technology – Cybersecurity)
   - SB 112/HB 148 (Personal Information Protection Act – Revisions)
   - SB 231 (Public Health – Cyber Safety Handbook – Handbook Development and Publication)
   - SB 351 (State Government – Protection of Information – Revisions (Maryland Data Privacy Act)
   - HB 425 (Criminal Law - Crimes Involving Computers)

Mr. Venkatraman added that SB 69 and SB 49/HB 38 were complementary. He observed that SB 49 clarified and codified the role of DoIT with respect to other branches of government and political subdivisions. SB 69 intends to codify the role of MEMA in working with DoIT and other state entities to enhance the preparedness and resilience of political subdivisions. SB 69 builds on what both DoIT and MEMA do well.

Senator Hester affirmed those comments as she joined the meeting. Mr. Khona commented that it made sense to give MEMA a specific cybersecurity mission. Given the convergence of IT and OT, there is a risk of physical disruption akin to other types of disasters that MEMA is asked to manage.

With respect to SB 231, Mr. Venkatraman observed that cyber-related behaviors were a rising public health issue and that raising awareness about safe Internet, social media, and technology usage among students, teachers, and other public school employees was important. A collateral benefit is that the training might also raise awareness of cybersecurity as a career and indirectly support other talent pipeline building efforts.

Dr. Joshi strongly commended the bill. As both a professor of computer science and a parent, he is very aware of the problems and the need for training. He would be happy to testify in support of the bill as a concerned parent.

Beyond the bills that were responsive to Council recommendations, Senator Hester briefly summarized two other bills that she wanted the subcommittee to be aware of:

- SB 66/HB 97 (Department of Housing and Community Development - Office of Digital Inclusion - Established (Digital Connectivity Act of 2021)
- SB 412/HB 84 (Right to Repair)

Senator Hester then turned to the core agenda item, which was the cyber workforce development bill. A draft of the bill was not available, but Mr. Venkatraman had distributed a draft outline of the bill's key components. The draft bill was expected by the end of the month. In summary, the bill would do several things:

- It would pre-program $25 million of any future federal workforce development funds for cybersecurity workforce development.
- It would establish a workforce development grant fund to be constituted from MHEC scholarship appropriations that are unspent each fiscal year and would otherwise revert to the General Fund.
- It would designate the Department of Commerce as the administrator of the grant program.
- The grant program would:
  - o Provide scholarships to individuals in training and education programs created or identified under by the program.
  - o Seed funding for identification and screening programs for employees with potential for upskilling into cyber/IT job roles
  - o Seed funding for apprenticeships at small cybersecurity firms, non-profits, and County Governmental Entities (50 employees or less)
- The grant recipient would be eligible for up to 20% of the available fund for administration and demand-side planning for each of three years.
- Eligible to apply would be a cybersecurity industry association in the State.

Mr. Petersen observed that the bill should be careful in the language that it uses when targeting training. He volunteered to send Mr. Venkatraman language that the federal government uses. He also noted that NICE does not conceptualize cyber as a sector; that IT and cyber cut across all sectors and that all sectors suffer from the skills gap.

Ms. Nelson asked whether the grant-funded training would focus on cyber narrowly or broadly understood. Mr. Smith advocated for training to be broadly defined to encompass both defensive and offensive operations.

Mr. Khona was very supportive of the bill. He pointed out that the program would help smaller firms get the talent that they need. With the talent shortage, smaller firms find it difficult to compete with larger firms for talent.

Senator Hester stated that she expected the bill be heard later in February. She mentioned that anyone interested would be able to submit testimony. With no further business, the meeting was adjourned at 6:15 pm.

[Note: These minutes were approved at the 14 July 2021 meeting of the subcommittee.]