Summary

Maryland Cybersecurity Council Meeting
November 10, 2015, 10:00 - 11:18 AM
University of Maryland University College
Adelphi, Maryland

Council Members Present or Represented

Council Chair, The Maryland Attorney General Brian Frosh, Senator Susan Lee, Donald Fry, Victor McCrary, Philip Quad, Judi Emmell, Shiva Azadegan, Zuly Gonzalez, Jonathan Powell, Anton Dahbura, Mark Augenblick, James Foster, LaToya Staten, Larry Letow, Brian Israel, Michael Greenberger, Clay House, Henry Muller, Tony Lisuzzo, Bel Leong Hong, Sue Rogan, David Engel, Phil Schiff, Rajan Natarajan, Patrick O'Shea, Joseph Morales, Howard Feldman, Steve Tiller, Joseph Haskins, Jonathan Katz, Robert Day, Jonathan Prutow, Paul Tiao, Carl Whitman, David Anyiwo, Jayfus Dowell

Others Present:
Amjad Ali (University of Maryland University College), Zenita Wickham Hurley (Office of the Maryland Attorney General), Sachin Bhatt (Office of the Maryland Attorney General), Michael Lore (Senator Lee's Office) and Karen Morgan (Maryland Department of Legislative Services)

Council Meeting

Department of Information Technology Cybersecurity Efforts

David Garcia, Secretary of Information Technology, stated that when Governor Hogan came into office, the administration took inventory of how it was protecting not just the government, but also the individual data of citizens collected by the government.

The state is fortunate to have such a large and sophisticated community of cybersecurity organizations within it, he said, and the goal now is how to build that community to include all state agencies, industry partners and even the school system to include cybersecurity in the curriculum.

The challenge, he said, is to tie together all of the dissimilar hardware and operating systems with dissimilar anti-virus technology into a standard baseline that can be defended.

All of these entities, he said, need to have closer bonds, have joint exercises, and train together to make Maryland safer.

Mission and Purpose of the Council

The Council had its picture taken to commemorate its first meeting.

Sen. Lee acknowledged the role that UMUC played in setting up the meeting as well as Zenita Hurley and Sachin Bhatt of the state Attorney General's office for their role.

The key to cybersecurity is making sure the laws keep up with the technological changes, she said. The Council came about because of the federal government's failure to pass any meaningful cybersecurity legislation. The Maryland Assembly enacted its own legislation in 2011. It created a cybersecurity commission that helped the Assembly pass bills that protected state databases and created a notification system to alert everyone to any breaches.

All of the bills have been piecemeal, she said, but the threat requires a comprehensive approach that brings all of the stakeholders together. That led to the creation of the Council that would fall under the jurisdiction of the state attorney general.

Its role, she said, is to conduct reviews and risk assessments of critical infrastructures vulnerable to cyber attacks that are not covered under federal law or federal executive orders. These would come up with best practices and standards following what NISC has recommended.

She welcomed federal partners in this because the state cannot do it alone.

Among the subcommittees she would like to see included in the Council are Cyber Legal Strategy, Structure and Practices Workforce Education and Development, Marketing and Partnerships.

In the absence of the Attorney General, Chairman Fry can designate who is assigned to each committee based on expertise and interests, she said Members can serve on more than one subcommittee.

She said the new Council would hold a reception at the beginning of the legislative session to help educate legislators about the needs for cybersecurity legislation. Dr. Vint Cerf has agreed to be at the reception as he is being honored by the Assembly.

<u>UMUC Cybersecurity Programs</u>

Dr. Amjad Ali stated that the Council that UMUC has responded to the shortage of cybersecurity professionals by creating seven different cybersecurity programs at the undergraduate and graduate levels. Since 2010, UMUC has graduated more than 4000 cybersecurity professionals and currently more than 8,000 are enrolled in those programs.

He said the university has formed a cyber team called the Cyber Padawans that has won several state, national and global competitions, including the 2014 Cyber Olympics in Barcelona, Spain.

In developing the cyber programs, UMUC worked with industry leaders to make sure the programs included not just technical aspects, but also human, legal, policy and ethical aspects associated with addressing cybersecurity problems in a more comprehensive and systematic manner. He indicated that the Council should take into considerations all these factors in their recommendations to strengthen the critical infrastructure of Maryland.

Establishing Subcommittees

Mr. Frosh asked for input about Council subcommittees. The ones listed in the agenda are tentative. He said the Council staff would take recommendations made today to come up with a list of subcommittees and circulate it to Council members so they can decide on which they want to serve.

Subcommittees on the list were Cyber Legal Strategy, Cyber Structure and Practices, Cyber Workforce Education and Development, Cyber Marketing and Partnerships.

Mr. McCrary suggested a subcommittee to study ongoing research activities in the state.

Mr. Tiao asked that a detailed description of each subcommittee be provided before people were required to make a decision. He said cyber marketing could be interpreted in different ways. He suggested a subcommittee on the structure and state of cyber security.

Mr. Tiao also suggested that the scope of the Council should be broadened so that it is not just about cyber intrusions, but also about cyber-enabled crime such as child pornography, cyber fraud.

Mr. Israel suggested a subcommittee on how to respond to cyber disaster.

Ms. Leong Hong said it would be good for the Council to shine a light on rapidly developing cyber technologies. It also might want to focus on what to do after an attack.

Mr. Letow suggested exploring ways of providing funding to attract private enterprise to enter the market in cybersecurity.

Mr. Foster cautioned that little money has come to Maryland in joint ventures beyond a few large government contractors.

Mr. Quad said the Council should not think that each organization or infrastructure should be strong enough to take on the Russians or the Chinese. Cybersecurity is a team sport, he said, and routine sharing of information on incidents is important. The Council should pilot some innovative technologies in one or two critical local infrastructures and then pass the lessons on to others. He also stressed the need for practicing how to get business back to normal after an attack.

Mr. Feldman emphasized the need for training at small companies so that employees do not inadvertently cause the conditions that allow for a successful cyber attack.

Mr. Muller said the Council also should consider how to use cyber technology to modernize state and local police to operate more efficiently with first responders.

Mr. Dahbura said that the Council should identify what other states and organizations are doing so that it does not try to reinvent what already exists.

Mr. Frosh said that based on these comments, the Council staff would send members subcommittees list that tries to incorporate these thoughts. Then, members should respond with

which subcommittees interest them. From there, the Council will designate chairs of each subcommittee.
The subcommittees will serve as the building blocks for the Council.

Ms. Leong Hong suggested that the reports of the old Commission should be made available to the new Council members to see what work has been done.

Mr. Foster cautioned that Council members should be made aware of the Freedom of Information Act and what could be made public.

Mr. Tiao suggested that experts who are not on the Council should be encouraged to be advisers to the subcommittees. He said if the subcommittees are able to put together proposals that are passed by the Assembly, Council members will be inspired to work even harder.

Mr. Quad asked the chair what success would look like?

Mr. Frosh responded that the Council will advise the government and the private sector on how to strengthen cybersecurity.

Senator Lee said the former commission had helped create several series of laws that were the first for the state. She said the purpose of this Council is to build on that momentum to come out with substantive deliverables for the state in protecting cyber and advancing it.

The meeting concluded at 11:18 a.m.