Summary
Maryland Cybersecurity Council Meeting
October 18, 2016
10:00am – 12:00pm
University of Maryland University College
Adelphi, Maryland

Council Members Present or Represented
John Abeles, Secretary Garcia (Charles Ames), David Anyiwo, Robert Day, Jayfus Doswell, Anton Dabura, Russ Strickland (Terry Thompson, Charles Eby), Judith Emmel, Don Fry, Michael Greenberger (Markus Rauschecker), Joseph Haskins, Clay House, Dr. Anupam Joshi, Senator Susan Lee, Bel Leong-Hong, Delegate Mary Ann Lisanti, Ken McCreedy, Joseph Morales, Henry Muller, Rajan Natarajan, Jonathan Powell, Jonathan Prutow, Martin Rosendale, Sue Rogan, Major General Linda Singh, Paul Tiao, Steve Tiller, Pegeen Townsend,

Staff, Invited Guests and Contributors Attending
Howard Barr (Office of the Attorney General), Colonel Shawn Bratton (175th Air Wing, Maryland National Guard), Terri Hayes (Contributor), Zenita Hurley (Chief Counsel, Civil Rights and Legislation, Office of the Attorney General), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Dr. Greg von Lehmen (Council Staff, UMUC).

Council Meeting (Quorum present: 28 of 51 members)

Remarks by Mr. Don Fry (Serving as Chair for Attorney General Frosh)

Mr. Fry opened the Council meeting by welcoming everyone and by thanking the Council and its contributors on behalf of Attorney General Frosh. He made several announcements:

- Council staff changes. He thanked outgoing staff members for their service. New staff are Howard Barr (OAG) and Dr. Greg von Lehmen (UMUC), replacing Sachin Bhatt (OAG) and Dr. Amjad Ali (UMUC), respectively.
- Due date for subcommittee drafts. Subcommittee drafts are due April 15, 2017. These will form the July 1, 2017 report on Council activities required by statute.
- Upcoming cyber-related events. He reminded the Council of CyberMaryland (October 21-22) in Baltimore and of the Council's own Public Policy Forum on Cybersecurity (December 6) hosted by UMUC.

Following the announcements, the minutes for the May 18, 2016 meeting were opened for discussion. After full consideration and a motion duly made and seconded, the minutes were unanimously approved.

Mr. Fry then turned to the subcommittee chair reports. He noted that in its *July 2016 Interim Activities Report*, the Council had identified many initiatives that were prioritized after review by the Attorney General and in discussions with the subcommittee chairs. Mr. Fry noted that the *Report* is a public document that can be found online. The subcommittee reports are summarized below.

Senator Susan Lee, Subcommittee for Law, Policy and Legislation

Cyber First Responder Reserve. The subcommittee continues to accumulate information to shape the concept of a reserve. This information includes the activity of the National Guard's cyber units and the existence of the Maryland Defense Force that works with the Guard. It also has included discussions with MEMA.

MEMA has noted that its role in relation to a cyber first responder group would be the same as it is now with respect to other groups involved in an emergency response, namely MEMA would be the coordinating agency, not the lead agency. DoIT would be the lead agency in an incident response. DoIT is actively working on a full incident response plan and MEMA is participating in that effort and will share the plan with the subcommittee. When a first responder group is activated, it must be integrated into the plan.

Other points pertinent to establishing the cyber first responders reserve.

- If the emergency involved private critical infrastructure, there would need to be coordination with the private sector, since the State does not have direct control of private entities.
- The State does not have a list of specific public and private infrastructure entities falling with the 16 US DHS critical infrastructure categories.
- If a first responder reserve is authorized and formed, MEMA will need additional funding to manage or coordinate it. Now 75% of MEMA's funding is from the federal government.
- MEMA and DoIT have exercised a cyber emergency (table top) but more exercises will follow to identify gaps in communication, coordination, equipment and technical talent to refine the plan and better prepare for its execution.

Data breach legislation. Senator Lee noted that the commercial breach statute—the Maryland Personal Information Protection Act (MPIPA)—and the State breach law need to be updated. She had in fact introduced the bill that now applies breach notification provisions to State and local government entities, although in the end the legislative and judicial departments were excepted. She had also introduced a bill in 2013 to update MPIPA, although it did not pass. The updates are twofold which the subcommittee proposes to address comprehensively rather than in piecemeal fashion:

- Revise the definition of personal and private information. Changes in technology now result in other types of personal identifying information to be collected, such as geolocation and biometric data. The definitions in both statutes should be adjusted to reflect this fact.

- Extend the State data breach law. Both the legislative and judicial departments hold substantial sensitive personal data and should also be encompassed by the provisions now covering other State agencies.

Senator Lee mentioned that Michael Greenberger, Professor of Law and Director of CHHS, Markus Rauschecker, Deputy Director of CHHS, and Mr. Howard Feldman are assisting the subcommittee with the bills that would provide these updates.

Other legislative recommendations of the subcommittee. Senator Lee indicated that the subcommittee would like to pursue in the following:

- Reintroduce a bill that would require DoIT to adopt the NIST Cybersecurity Framework (CsF). Originally devised for the critical infrastructure sectors with input from government and industry, it is now recognized as a flexible and effective guide for enhancing cybersecurity. A bill requiring DoIT to use the CsF has passed the Senate previously but not the House of Delegates
- Provide a private right of action in the case of hacking attacks. Senator Lee noted that California is one example of a state that has adopted legislation of this nature.

Charles Ames for Secretary Garcia, Chair, Cyber Incident Response Subcommittee

Mr. Ames made a presentation that offered an overview of DoIT's efforts to improve its security posture. He made the following key points:

- Over the last six months, DoIT has systematically been evaluating state agencies against the respected CIS Critical Controls and the NIST Cybersecurity Framework to assess their maturity and the risks they present and to identify the quick wins.
- Concurrently, DoIT has rewritten all its policies that concern cybersecurity itself. He expected that soon they will be approved by the Secretary and published for reference by procurement offices and local governments.
- Part of DoIT's security strategy is leveraging the cloud and the security services offered by the cloud provider. The policies that DoIT has revised will be used by the provider and has accelerated the implementation.
- There have been improvements in network monitoring/detection and in perimeter defense that have helped the State with a variety of compliance requirements.
- In addition, DoIT also has an effort underway to identify all endpoints within the agencies and to start addressing their security.

Mr. Ames concluded by offering an environmental scan of the threats (referencing the Ukraine, SWIFT, and the DNC breach, and risks posed by the Internet of Things), legislative trends (will there be a national breach law?), and some of the challenges that DoIT faces with all IT organizations, such as the shortage of people with the needed security skills.

Markus Rauschecker for Michael Greenberger, Chair, Critical Infrastructure Committee.

Mr. Rauschecker indicated that due to other business Professor Greenberger was not able to participate in the Council meeting and conveyed his regrets. He identified three lines of effort by the subcommittee:

- The first is to establish an educational infrastructure that provides resources (information on issues, frameworks, standards, best practices, threat sharing mechanisms) to Maryland critical infrastructure sectors and other stakeholders in the State. Mr. Rauschecker noted that there are many resources available through the federal government, the State of Maryland and a variety of other entities. The challenge is that there is no one place where they are catalogued and easily accessible. This is particularly a problem for small and medium-size entities that do not have large dedicated cybersecurity teams. The recommendation would help address this challenge. Mr. Rauschecker indicated that other subcommittees were looking at the same issue and that developing a portal of some type would be a collaborative effort.
- The second it to identify the critical infrastructure sectors that are at greatest risk of cyber attacks and need the most enhanced cybersecurity measures. The US Department of Homeland Security of course has identified 16 critical infrastructure (CI) sectors, but the State could benefit from a better inventory of its CI infrastructure and which sectors need more support. This effort would also recognize the interdependencies among sectors, including geographical interdependencies. For example, every sector is dependent on the electrical grid and Maryland's power can be affected by interruptions in other states.
- The third is to encourage critical infrastructure and other private sector entities to conduct risk assessments and to provide information concerning resources and tools to help entities conduct risk assessments. Most critical infrastructure is in private hands, although there are some, like water treatment plants, that may be operated by local governments.

In response to the report-out, Mr. Rauschecker was asked how widely the CsF was adopted in and outside of the CI sector, given it is a voluntary framework. He responded that adoption had momentum in the private sector where it has become viewed as one way to show good faith effort to avoid legal liability for breaches. He also noted that the federal government requires all contractors to have a cybersecurity program of some sort. Other comments made by members of the Council pointed to the importance of the NIST risk assessment framework and other NIST resources as valuable tools.

Dr. von Lehmen for Dr. Jonathan Katz, Chair, Education and Workforce Development Subcommittee.

Dr. von Lehmen noted that Dr. Katz very much regretted that he could not join the Council meeting and that Dr. Katz had asked him to make the subcommittee report since he had attended its most recent meeting.

Dr. von Lehmen indicated that the Attorney General had approved three subcommittee recommendations for action and provided the update below on their status:

Assess cyber workforce demands in Maryland. The aim of this initiative is to help inform educational programs in cybersecurity to keep pace with changing needs. The subcommittee has paused its effort in this area because the recommendation may be achieved by a project funded by NIST through the National Initiative of Cybersecurity Education (NICE). The purpose of the project is to compile current and granular information about the cybersecurity job requirements that employers are looking to fill in every state and locality. The first iteration of the data will be available on the web and previewed at the NICE Annual conference in November. The subcommittee will assess whether the data achieves its goal.

Develop a scholarship for state service proposal. The subcommittee believes that such a program might help State agencies with their workforce needs in cybersecurity. It has collected information about the federal scholarship for service program and is currently considering how Maryland might be able to fund a similar program for Maryland.

Support K-12 computer science pipeline-building efforts. The subcommittee has just begun work on this recommendation. It is aware that MSDE is making significant strides in this area and has obtained the support of a liaison to help the subcommittee understand the full range of the Department's pipeline building efforts before developing proposals that MSDE might welcome.

Dr. von Lehmen was asked about the status of computer science training in K-12, and he mentioned the Career and Technical Education (CTE) programs in this area that are offered by public high schools. But he noted that a challenge is finding teachers who can offer computer science courses. Another member of the Council pointed out that the University of Maryland, College Park, is working with the State under an NSF grant to train computer science teachers. Other comments were that computer science is considered 'shop'—and not science—in schools creating a disincentive for students to take the courses and that well-equipped labs as well as trained teachers is a challenge.

Bel Leong-Hong, Chair, Subcommittee on Economic Development

Ms. Leong-Hong noted that the charter of the subcommittee is to find ways to attract, grow and retain cyber-related businesses in Maryland. There are three recommendations that the subcommittee has organized around:

Map the lifecycle of a technology-oriented firm. The subcommittee has identified several models with the idea of understanding the needs of these firms at each stage in their development.

Development of an asset map for Maryland. The objective is to comprehensively identify what resources the State offers for cyber-related firms and how these resources map from start-up through maturity.

Incentives to support the growth of the State's cyber economy. The subcommittee has formulated proposals concerning procurement incentives, the extension of the employer

clearance tax credit, and a one-time income tax credit to attract cybersecurity professionals to Maryland.

Sue Rogan, Chair, Public Awareness and Community Outreach

Ms. Rogan was the final chair to report out. She updated the Council on the cybersecurity repository the subcommittee is creating and hopes to launch by July 1, 2017. There are many collections of information on cybersecurity covering a vast range of topics. The subcommittee's goal is to create one web-based portal where these other resources can be collected and catalogued for easy use. This project may link to initiatives of other subcommittees which aim to create libraries of resources for specific audiences. The Maryland Department of Information Technology (DoIT) has offered to host the repository.

With Ms. Rogan's report, Mr. Fry thanked the chairs and their committees for their work, recognizing the extensive and substantial nature of the initiatives underway. He then introduced the Council's guest speaker, Colonel Shawn Bratton, Commander of the 175th Wing Cyber Operations Group of the Maryland National Guard. Colonel Bratton was invited to inform the Council of what cybersecurity capabilities his unit and the Maryland National Guard in general bring to the nation and to the State.

Colonel Bratton's presentation provided an overview of the State's Military Department, the work of his operations group, and lessons learned from the Baltimore riots. Key take-aways for the Council were:

- The Maryland National Guard leads in its cyber offensive, defensive and intelligence capabilities among state Guard units. In addition to the 175th Wing Cyber Operations Group, the Maryland Army National Guard also has a battalion with cybersecurity capabilities.
- The Guard's cyber capabilities support CYBERCOM and are available to the Governor for action within Maryland.
- Where the cyber operations group would be involved, the best use of the Guard in a cyber emergency is not to be in the networks of other entities but to be shoulder-to-shoulder with their operators to advise them.
- As a result of the Baltimore unrest, the Guard learned that it needed to develop the appropriate authorities and cross-agency relationships to work effectively in support of the State's other cyber resources. The Guard has made substantial progress in these areas.
- To help address challenges in policy, needed tools and other areas, Major General Singh, the Maryland Adjutant General, is leading the creation of a Cyber Center of Excellence with representatives from universities and community colleges across the State.

Colonel Bratton's presentation was followed by questions about the cyber capabilities of other state National Guard units, whether senior Guard officers seek additional education and what type, and what cyber jobs the Guard trains graduates right out of high school to do.

Major General Singh followed Colonel Bratton with remarks of her own. She emphasized that building cyber capabilities within the Guard take time and are expensive. She noted that DoD and the Guard are looking at better ways of screening young people interested in cyber to improve selection, increase training throughput and reduce costs. Finally, she left the Council

with the message that developing the talent needed by the Guard and civil society requires teaching young people the importance of personal responsibility, leadership and ethics. The Maryland National Guard is very active in answering invitations to go into schools to talk about these things. The Guard is working to expand its outreach program by involving its retirees.

Mr. Fry expressed the Council's appreciation to Colonel Bratton for a very substantive presentation and to Major General Singh both for making him available and for her remarks. There being no further business on the agenda, on behalf of Attorney General Frosh Mr. Fry again thanked the Council, its contributors, and the staff for their work.

Meeting adjourned at noon.