Summary
Maryland Cybersecurity Council Meeting
June 1, 2017
10:00am – 12:00pm
University of Maryland University College
Adelphi, Maryland

Council Members Present or Represented (19)
Attorney General Brian Frosh, Secretary Leahy (Charles Ames), David Anyiwo, Delegate Ned Carey, Judith Emmel, Michael Greenberger, Brian Israel, Brian Corbit (Ronald Kaese), Senator Susan Lee, Henry Mueller, Bel Leong-Hong, Delegate Mary Ann Lisanti, Ken McCreedy, Jonathan Powell, Sue Rogan, Colonel Mathew Dinmore (Major General Linda Singh), Paul Tiao, Rajan Natarajan, and Pegeen Townsend.

Staff, Invited Guests and Contributors Attending
Zenita Hurley (Chief Counsel, Civil Rights, OAG), Tiffany Harvey (Chief Counsel, Legislative Affairs, OAG), Howard Barr (AAG and Principal Counsel, DoIT), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Markus Rauschecker (CHHS), Dr. Greg von Lehmen (Council Staff, UMUC).

Council Meeting

Remarks by the Attorney General

The Attorney General welcomed council members, contributors and other members of the public who were in attendance. He mentioned that his schedule would require him to leave before the meeting ended and that Ms. Zenita Hurley would step into the chair for him. He made two other announcements:

- Ms. Hurley would be stepping down as the liaison with the Counsel so that she could focus on her role as Chief Counsel for Civil Rights. Tiffany Harvey, the new Chief Counsel for Legislative Affairs, will step into the council liaison role. The Attorney General and the council thanked Ms. Hurley for her work and welcomed Ms. Harvey.
- The Attorney General announced two new members who have joined the council: Maryland Senator Bryan Simonaire and Tami Howie, CEO of the Maryland Tech council.

He called for the minutes of both the March 17, 2017, and October 18, 2016, meetings and asked if any members had objections to approving them. There being none, the minutes are considered approved.

He then outlined the purpose of the present meeting:

- The goal is to inform the council's activities report due to the General Assembly by July 1, 2017. He noted that it is essential to capture the council's accomplishments since 2015 and any new recommendations for the next two years.
- To allow plenty of time, no presentations have been planned. The agenda is dedicated to the subcommittee report-outs and the related discussion.
- "Thank you's" are in order to council members and to 'contributors' who have supported the subcommittees in their work. Much has been accomplished.
- The timeline to produce the report will be as follows:
    - By June 5 *at the latest*, a complete draft of the council's report will be circulated to council members for comment. The Attorney General asked that the council keep the distribution confidential and not share it outside the membership.
    - On June 15, the comment period will close. Thereafter, proposed revisions will be considered and the final draft will go through a process of review at OAG prior to the July 1 release of the report.

Subcommittee Report-outs

Senator Susan Lee, Co-chair, Law, Policy and Legislation Subcommittee

Senator Lee noted three significant accomplishments for Maryland citizens in the last session.:

The updating of the Maryland Personal Information Protection Act (MPIPA). SB 525/HB974 enlarged the category of personal information protected by the law to include biometric data, health records, email addresses in combination with login credentials, and various unique government identifiers in addition to the social security number. The law also clarified when breach notifications had to be made (no later than 45 days) in lieu of a more general reasonableness standard.

The provision of a one-time free credit freeze for consumers. SB 270/HB 212 strengthens the credit freeze as a protective measure by encouraging consumers to use it. Senator Lee emphasized that the credit freeze is more effective than credit monitoring: it is a proactive measure that consumers can take to reduce the impact of identity theft *before* it happens.

The extension of the tax credit to businesses for the cost of security clearances. SB 138/HB873 mitigates the cost of SCIFS and contributes to the growth of the cyber business sector in Maryland. The bill was responsive to a request by the council's Economic Development Committee to the Law, Policy and Legislation Subcommittee.

Looking ahead to the next two years, Senator Lee said that her subcommittee proposed to:

- mature the cyber first responders' corps concept into legislation (2016 Recommendation #1)
- update the state breach statute to align its protections with MPIPA's and to extend the breach notification requirements to personal information held by the judicial and legislative branches
- make additional enhancements to MPIPA, such as extending the breach protection to small businesses whose credit card information may be compromised
- devise legislation that would require vendors to code IoT devices in a manner that would clearly indicate to consumers what level of security (if any) the devices incorporated
- craft a bill that would preclude the sale of browsing history by ISPs without consumers' express consent. (Senator Lee mentioned that this is in response to the recent roll back of an FCC regulation by the Congress.)
- introduce legislation that would give consumers the right to inspect and correct data profiles held by data brokers about them and mandate a portal where any such firm holding Maryland citizen data must list itself and its contact information for said purpose
- reintroduce ransomware legislation, specifically either creating a ransomware definition in the criminal extortion statute, or creating a new code section with an increased penalty for extortion levels below the general extortion threshold
- finally, to reintroduce right of civil action, enabling businesses to sue former employees whose conduct is the proximate cause of a breach of personal identifying information.

In highlighting the progress on the subcommittee's recommendations, Senator Lee expressed appreciation especially to Professor Greenberger, Marcus Rauschecker, Howard Feldman, Paul Tiao and Michael Lore for the work on MPIPA and the strong support of OAG for both the changes in MPIPA and the credit freeze legislation. She also endorsed Professor Greenberger's proposal at the council's March meeting to organize a series of briefings for legislators to better inform them about the need for ransomware legislation.

Mr. Tiao pointed out that Senator Lee did the heavy lifting on much of the successful legislation last session. As a member of Senator Lee's subcommittee and a practicing attorney in the field of breach law, he also noted that ransomware is the new plague, eclipsing the retail data breach as the headline. Its elevation as a public issue creates a window of opportunity for legislation to address it. Ms. Leong-hong pointed to the ransomware attacks on hospitals as an example and strongly supported the idea of legislative briefings, suggesting that they start earlier than the legislative session if possible. Senator Lee indicated that the health and judicial proceedings committees would be key.

Ms. Townsend observed that Maryland hospitals are very focused on the ransomware threat and that they have been communicating and working effectively together to minimize its impact. She also recommended that for the bill concerned with the sale of consumer browsing history, the

stakeholders be engaged before the bill is submitted to the General Assembly. Senator Lee expressed appreciation for the suggestion and stated that such was her intention.

Professor Michael Greenberger, Chair, Critical Infrastructure Committee

Professor Greenberger thanked Senator Lee and Michael Lore especially for their efforts in the last session. In his view, the successful legislative initiatives coming out of the Law, Policy and Legislation Subcommittee would by themselves demonstrate the importance of the council to Maryland. He stated that getting good ideas into law is often iterative and that the efforts of the last session that did not produce legislation will support efforts in the next.

For his comments, Professor Greenberger referred to the substantial report that his subcommittee produced to inform the larger council report due in July. In its last two years, the subcommittee has focused on a) identifying cybersecurity resources that will be useful to small- and medium-size enterprises, including critical infrastructure (CI) operators, and b) finetuning the list of CI sectors for attention along with the key principles that should guide the subcommittee's work in this area.

Resources. He noted that this effort complements the work of the Community Outreach Subcommittee to develop a publicly accessible portal with DoIT to promote awareness and provide basic cybersecurity tools for citizens and smaller organizations. Specifically, his subcommittee has identified and categorized a substantial list of resources for smaller enterprises that cannot afford private assistance. These fall into two categories.

- One offers general resources. Included are NIST special publications and other resources that address a variety of topics: general cybersecurity awareness, information sharing through information sharing and analysis organizations (ISAOs), cybersecurity frameworks, including the NIST *Framework;* critical infrastructure tools for cybersecurity, cyber risk management, and cyber workforce development and training.

- The other category is dedicated to risk assessment. This is composed of an extensive compilation of previous CI assessments and risk assessment methodologies.

Priority CI Sectors. Professor Greenberger acknowledged the list of 17 CI sectors identified by DHS, but the subcommittee will focus on a smaller subset of those serving Maryland. The two key principles that will inform the subcommittees risk assessment efforts are the interdependency of CI sectors and the regional or multistate character of CI affecting Maryland. The electric grid is an example. All CI sectors are dependent upon it, and Maryland's power generation is part of a larger regional network.

For the next two years, the subcommittee intends to add to the repository of resources that it has initially compiled, work with the Cyber Operations and Incident Response Subcommittee on supporting information sharing activities, and recommend legislation to the council that would emphasize cybersecurity in CI licensing and other areas.

Mr. Charles Ames, Director of Cybersecurity, DoIT, for Secretary Michael Leahy, Chair, Cyber Operations and Incident Response Subcommittee

Mr. Ames also spoke from his subcommittee's report covering the last two years and proposing initiatives for the next two. He observed that the threat landscape is moving very fast and that it is difficult for the state to stay in front of threats. Ransomware is a good example of how fast the landscape changes. In 2015, ransomware was a footnote. A recent report indicated that in 2016, globally, there were 638 million ransomware attacks. Two years ago, data exfiltration to embarrass people with information was not a practice. Now it is. Then there are the APT vectors that are always morphing and probing network defenses.

He mentioned that the chief accomplishment of the last two years was the creation and validation of the state's cyber response plan. This is a charge to the council under its enabling statute and was accomplished as a cross-agency effort involving DoIT, MEMA, the Military Department, and other agencies. The plan has been cross-exercised two times this year, including as part of the recent Cyber Guard exercise.

In the next two years, the subcommittee recommends advancing the idea of a structure in Maryland that could both provide salient threat information to citizens and small businesses and offer assistance when these fall victim to some sort of attack. Salience is key. There are numerous threat feeds, and the most relevant threats need to be highlighted. There also needs to be a place where citizens and enterprises too small to fend for themselves can go for help. Right now, the phone calls come to DoIT which does its best to assist, but its resources are limited too. For example, it does not have a 24/7 SOC and is supported at times by a call center with on-call resources only.

The other major recommendation of the subcommittee is to support an increase in state funding of CND. Maryland's current investment in its named cybersecurity function (under $5 million per year) places it near the bottom of the states. There has been progress in the last two years. But there is considerable ground to make up and much that continues at risk.

While not within its charge, the subcommittee asked the council to consider changes in Maryland government procurement policy to require higher cybersecurity standards for IT equipment and third-party suppliers of services. DoIT has scanned a number of vendors that service the state and found their security wanting. Example: there was a case of a county recently that was hit by ransomware, and services were knocked completely offline for several days. DoIT was able to mitigate the attack before key assets were lost. Still, it took the county four or five months and significant expenditures to recover. Changes in procurement policy would mitigate some of these problems.

In response to Mr. Ames' comments, Mr. Tiao asked if the state is leveraging InfraGard. Mr. Ames agreed that there are advantages to InfraGard, not the least of which is that members must

have a national background check. But there are challenges too. In an emergency, it is not known who will show up with what skills, and the state presently does not have plans in place to use InfraGard members. Mr. Tiao acknowledged the problems but noted that InfraGard is making some changes and that it might be a good organization engage.

About state funding on cybersecurity, the Attorney General asked Mr. Ames what investment is needed to reasonably secure the state. Mr. Ames indicated that sustaining a $12.5 million a year investment would meet that goal. This would not place Maryland in the first tier of states investing heavily in cybersecurity, but it would be a significant improvement. Mr. Ames noted that the current budget for DoIT's cybersecurity function is less than $5 million and put Maryland in the bottom tier of states investing in cyber.

Delegate Lisanti strongly supported the suggestion that the state strengthen its procurement policies to require IT equipment and vendors providing services to meet higher cybersecurity standards. She viewed it as low hanging fruit and asked whether this could be accomplished as a policy change by the executive branch or whether it would require legislation. Mr. Ames said that the executive branch could institute a policy change, but it would not affect the legislature or the judiciary. Professor Greenberger indicated that legislation might be required, although he would have to research the question. Delegate Lisanti asked that the rationale for the procurement change be developed and volunteered the legislative delegation to help identify the means. There were no objections to adopting the suggestion as a recommendation.

Ms. Sue Rogan, Chair, Community Outreach Subcommittee

As background, Ms. Rogan pointed out that her subcommittee consists of representatives from postsecondary education, small businesses and a nonprofit organization. Consistent with the council's 2016 *Initial Activities Report*, her subcommittee's focus has been on developing a repository for resources that would be helpful to citizens, small business, and other small organizations. The subcommittee has worked with the realization that this repository would also hold the resources that would be developed through the Critical Infrastructure Subcommittee. DoIT has volunteered to help create the repository itself.

Ms. Rogan previewed a mock-up of the repository for the council. The site would include categories that would align the content with specific audiences and include tips that would be changed periodically. She noted that there must be a protocol for vetting and adding new resources to the site and the assignment of responsibility to maintain the repository. Ms. Rogan also noted that the subcommittee had developed a list of organizations to which the repository could also be linked to extend its visibility.

Mr. Ken McCreedy suggested that the repository include CAMI and the cybersecurity asset map that the state Department of Commerce is developing. Both would be resources important to capture. Ms. Rogan indicated that CAMI is included as a resource and looked forward to adding the cyber asset map.

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

Dr. von Lehmen expressed Dr. Katz's regrets for not being able to participate in the council meeting. He summarized the subcommittee's progress and plans on his behalf. He noted that of the six recommendations made by subcommittee in 2016, it had made progress on two, closed out one and would continue to pursue the other three. Specifically:

Enhancing K-12 computer science and cybersecurity education. The subcommittee arranged a liaison from the Maryland State Department of Education (MSDE) to help it understand what the state's public schools were doing or had planned in these areas. MSDE has been working to enhance computer science and cybersecurity education through key curricular initiatives, including a cybersecurity resource toolkit for teachers, the creation of computer science and cybersecurity CTE programs, and the planned adoption in some form of the forthcoming K-12 standards for computer science education to be published by the Computer Science Teachers Association (CSTA). Among the biggest challenges are funding for equipment and teacher training.

Cybersecurity scholarship for service. The subcommittee has recommended that the state emulate the NSF scholarship for service program and has familiarized itself with the details about how the program works. The subcommittee is now investigating existing state scholarship programs that might be 're-programmable' for cybersecurity scholarships for service.

Study cybersecurity workforce skill needs in Maryland. The subcommittee had two goals, namely to identify: a) an accepted definition of cybersecurity to anchor any estimate of cybersecurity workforce needs in Maryland, and b) an accepted source of granular information about required roles and skill sets. As a result of its due diligence, the subcommittee satisfied itself that this recommendation had been overtaken by work done by NIST and recommended that it be closed. Specifically, NIST/NICE is updating its National Cybersecurity Workforce Framework—increasingly accepted as the authoritative definition of cybersecurity as a field—and has also funded the launch of a tool that provides granular information about open cybersecurity positions by state, region and the nation (Cyberseek).

The three initiatives that the subcommittee would continue to pursue are resources for computer science departments, transition path for community college graduates, and increased funding for academic research.

With respect to K-12 computer science and cybersecurity education, Mr. McCreedy mentioned that there is a Maryland firm that offers online education and certification preparation in cybersecurity and that this might be a resource for MSDE.

Ms. Belkis Leong-hong, Chair, Economic Development Subcommittee

Ms. Leong-hong noted that the subcommittee made recommendations to help the Maryland cybersecurity companies to grow and to remain in Maryland. These recommendations fell into two categories: a toolbox and incentives and investments.

Toolbox. The subcommittee had shaped the concept of an asset map that would identify resources that cybersecurity firms could use. As the subcommittee conceived it, these resources would be mapped to the business lifecycle to make the resources more accessible and impactful. However, the Maryland Department of Commerce had been considering such a tool in parallel with the subcommittee and had decided to fund it, effectively accomplishing this subcommittee initiative. This new tool will be previewed by Commerce at CyberMaryland 2017 this fall.

Incentives and investments. Consistent with its 2016 recommendation, the subcommittee has pursued three initiatives:

- Support for the extension of the tax credit for the cost of security clearances (SCIFS). This initiative was discussed with the Law, Policy and Legislation Subcommittee. Delegate Carey, a member of the latter subcommittee, sponsored HB 873 which passed the last session of the General Assembly.

- Extension of TEDCO's investment authority. The subcommittee examined the statute establishing TEDCO and considered whether it should be amended to make investment funds available for commercialization of new technology services; e.g. applications of blockchain to solve security problems. Its due diligence established that TEDCO had this authority already and that no changes in its statute should be recommended.

- Changes in state procurement law to ensure reciprocity. The subcommittee was concerned that Maryland firms did not enjoy the same preference in state procurements vis-à-vis nonresident firms that these firms enjoyed in their home states vis-à-vis Maryland firms competing for state contracts. With the assistance of the OAG staff member, the subcommittee that established that such statutory provisions exist.

In the two years ahead, the subcommittee will look at ways of incentivizing cyber professionals to relocate to Maryland and other tax and investment incentives to support the growth of the cybersecurity sector in state. In this connection, Ms. Leong-hong indicated that her subcommittee looked forward to working with the state Department of Commerce, the Cybersecurity Association of Maryland (CAMI), the Maryland Chamber of Commerce, and other entities. She thanked her subcommittee members for their efforts during the last two years and those nonmembers who had contributed to its work.

Mr. McCreedy noted that because there is not a NAICS code specifically for cybersecurity firms, it is difficult to know precisely how many such firms are in Maryland. The Department of Commerce is working with the Economic Alliance of Greater Baltimore to poll local jurisdictions to get a better data on this question.

Regarding the council's legislative agenda, Delegate Lisanti mentioned that she and Delegate Carey had debriefed after the last session about ways to make the process easier. She recommended that the council determine its legislative priorities with OAG early so that there is more time to educate members of the General Assembly about the bills and the specific issues that they are meant to address. Senator Lee concurred and noted that she had had similar conversations after the session ended.

Ms. Hurley thanked Delegate Lisanti and Senator Lee for their comments and added that might mean opportunities for council members to provide testimony. She also noted that the publication of the July 1, 2017 report to the legislature was a breakpoint of sorts, both closing the council's first two years but also looking ahead to the next two. She indicated that the staff would be reaching out to the members inquiring whether they wish to recommit. She expressed appreciation for the contributions of all the members and the hope that everyone would be able to continue.

Under 'other business', Dr. von Lehmen made some housekeeping comments about the open meeting requirements. He offered to assist subcommittees by managing the calendar invites and announcing the meetings in advance. While subcommittees must designate a physical meeting place to accommodate citizens who wish to join, a phone bridge can still be offered to subcommittee who may not be able to come to the announced location. He also offered access to a phone bridge facility if a subcommittee needed it.

Ms. Hurley announced that the next meeting of the council will be on October 25 from 10:00am – 12:00pm at UMUC. After calling for further business and hearing none, Ms. Hurley adjourned the council at noon.